

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関  
国際事務局(43) 国際公開日  
2004 年 11 月 18 日 (18.11.2004)

PCT

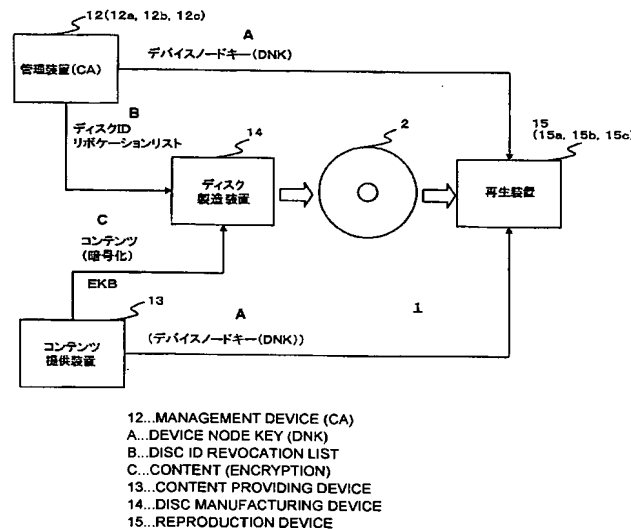
(10) 国際公開番号  
WO 2004/100154 A1

- (51) 国際特許分類: G11B 20/10, 20/12, 27/00, G06F 12/14, H04L 9/00, 9/32
- (21) 国際出願番号: PCT/JP2004/006324
- (22) 国際出願日: 2004 年 4 月 30 日 (30.04.2004)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:  
特願2003-125968 2003 年 4 月 30 日 (30.04.2003) JP
- (71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒1410001 東京都品川区北品川 6 丁目 7 番 3 5 号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 浅野 智之 (ASANO, Tomoyuki) [JP/JP]; 〒1410001 東京都品川
- (74) 代理人: 佐藤 隆久 (SATO, Takahisa); 〒1110052 東京都台東区柳橋 2 丁目 4 番 2 号 創造国際特許事務所 Tokyo (JP).
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY,

[続葉有]

(54) Title: DATA PROCESSING METHOD, PROGRAM THEREOF, DEVICE THEREOF, AND RECORDING MEDIUM

(54) 発明の名称: データ処理方法、そのプログラム、その装置および記録媒体



(57) Abstract: A management device (12) generates a plurality of different signature data by using its secret key and provides them as disc ID to a disc manufacturing device (14). The disc manufacturing device (14) manufactures a plurality of disc-shaped recording media (2) where the aforementioned disc ID are recorded. A reproduction device (15) reads out a disc ID from a disc-shaped recording medium (2) and verifies it according to public key data on the management device (12) before performing reproduction.

(57) 要約: 管理装置 12 は、自らの秘密鍵を用いて異なる複数の署名データを生成し、これをディスク ID としてディスク製造装置 14 に提供する。ディスク製造装置 14 は、複数の上記ディスク ID をそれぞれ記録した複数のディスク型記録媒体 2 を製造する。再生装置 15 は、再生装置 15 を再生する前に、ディスク型記録媒体 2 からディスク ID を読み出し、これを管理装置 12 の公開鍵データを基に検証する。



KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

添付公開書類:

- 国際調査報告書
- 請求の範囲の補正の期限前の公開であり、補正書受領の際には再公開される。

## 明 細 書

データ処理方法、そのプログラム、その装置および記録媒体

5

## 技術分野

本発明は、記録媒体を識別する識別データに係わる処理を行うデータ処理方法、そのプログラム、その装置および記録媒体に関する。

## 背景技術

10 光ディスクなどの記録媒体を用いてコンテンツを提供する場合に、その記録媒体が不正に複製されると、コンテンツ提供者の利益が不当に害される。

このような問題を解決するために、個々の記録媒体を識別するIDを各記録媒体に記録し、そのIDを基に不正に複製された記録媒体を特定するシステムが知られている。

15 しかしながら、上述した従来のシステムでは、記録媒体に記録されたIDが改竄されたものであるか、並びに正当な権限を有する者が生成したかを検証することができないという問題がある。

## 発明の開示

20 本発明は上述した従来技術の問題点に鑑みてなされ、識別データを基に記録媒体を管理する場合に、その識別データを不正に生成並びに改竄することが困難な形態で生成できるデータ処理方法、そのプログラムおよびその装置を提供することを第1の目的とする。

また、本発明は、上記第1の目的を達成するデータ処理方法、そのプログラム、  
25 その装置によって生成された識別データを適切に検証できるデータ処理方法、そのプログラムおよびその装置を提供することを第2の目的とする。

また、本発明は、上述した第 1 の目的を達成するデータ処理方法、そのプログラム、その装置によって生成された識別データを記録した記録媒体を提供することを第 3 の目的とする。

上述した目的を達成するために、第 1 の発明のデータ処理方法は、記録媒体を識別する識別データを生成するデータ処理方法であって、前記識別データの管理元の秘密鍵データを用いて、複数の異なる署名データを生成する第 1 の工程と、前記第 1 の工程で生成した前記複数の署名データを、前記識別データとして異なる複数の記録媒体にそれぞれ割当て第 2 の工程とを有する。

第 1 の発明のデータ処理方法の作用は以下になる。

10  まず、第 1 の工程において、前記識別データの管理元の秘密鍵データを用いて、複数の異なる署名データを生成する。

次に、第 2 の工程において、前記第 1 の工程で生成した前記複数の署名データを、前記識別データとして異なる複数の記録媒体にそれぞれ割当て第 2 の工程とを有する。

上記各工程はデータ処理装置が実行する。

15  第 2 の発明のプログラムは、記録媒体を識別する識別データを生成するデータ処理装置が実行するプログラムであって、前記識別データの管理元の秘密鍵データを用いて、複数の異なる署名データを生成する第 1 の手順と、前記第 1 の手順で生成した前記複数の署名データを、前記識別データとして異なる複数の記録媒体にそれぞれ割当て第 2 の手順とを有する。

20  第 3 の発明のデータ処理装置は、記録媒体を識別する識別データを生成するデータ処理装置であって、前記識別データの管理元の秘密鍵データを用いて、複数の異なる署名データを生成する第 1 の手段と、前記第 1 の手段で生成した前記複数の署名データを、前記識別データとして異なる複数の記録媒体にそれぞれ割当て第 2 の手段とを有する。

25  第 3 の発明のデータ処理装置の作用は以下になる。

まず、第 1 の手段が、前記識別データの管理元の秘密鍵データを用いて、複数

の異なる署名データを生成する。

次に、第2の手段が、前記第1の手段で生成した前記複数の署名データを、前記識別データとして異なる複数の記録媒体にそれぞれ割当てる。

第4の発明のデータ処理方法は、記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理方法であって、前記識別データの管理元の公開鍵データを用いて、前記識別データの正当性を検証する工程を有する。

当該工程はデータ処理装置によって実行される。

第5の発明のプログラムは、記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置が実行するプログラムであって、前記識別データの管理元の公開鍵データを用いて、前記識別データの正当性を検証する手順を有する。

第6の発明のデータ処理装置は、記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置であって、前記識別データの管理元の公開鍵データを用いて、前記識別データの正当性を検証する手段を有する。

第7の発明のデータ処理方法は、記録媒体を識別する識別データを生成するデータ処理方法であって、前記識別データの管理元の秘密鍵データとデータSとを用いて、前記管理元の公開鍵データを基に前記データSを復号可能な複数の異なる署名データを生成する第1の工程と、前記第1の工程で生成した前記複数の署名データの各々について、当該署名データと前記データSとを含む識別データを生成し、複数の前記識別データを異なる複数の記録媒体にそれぞれ割当てる第2の工程とを有する。

第7の発明のデータ処理方法の作用は以下になる。

先ず、第1の工程において、前記識別データの管理元の秘密鍵データとデータSとを用いて、前記管理元の公開鍵データを基に前記データSを復号可能な複数

の異なる署名データを生成する。

次に、第2の工程において、前記第1の工程で生成した前記複数の署名データの各々について、当該署名データと前記データSとを含む識別データを生成し、複数の前記識別データを異なる複数の記録媒体にそれぞれ割当てて。

- 5 第8の発明のプログラムは、記録媒体を識別する識別データを生成するデータ処理装置が実行するプログラムであって、前記識別データの管理元の秘密鍵データとデータSとを用いて、前記管理元の公開鍵データを基に前記データSを復号可能な複数の異なる署名データを生成する第1の手順と、前記第1の手順で生成した前記複数の署名データの各々について、当該署名データと前記データSとを含む識別データを生成し、複数の前記識別データを異なる複数の記録媒体にそれぞれ割当てて第2の手順とを有する。
- 10

- 第9の発明のデータ処理装置は、記録媒体を識別する識別データを生成するデータ処理装置であって、前記識別データの管理元の秘密鍵データとデータSとを用いて、前記管理元の公開鍵データを基に前記データSを復号可能な複数の異なる署名データを生成する第1の手段と、前記第1の手段で生成した前記複数の署名データの各々について、当該署名データと前記データSとを含む識別データを生成し、複数の前記識別データを異なる複数の記録媒体にそれぞれ割当てて第2の手段とを有する。
- 15

第9の発明のデータ処理装置の作用は以下のようになる。

- 20 先ず、第1の手段が、前記識別データの管理元の秘密鍵データとデータSとを用いて、前記管理元の公開鍵データを基に前記データSを復号可能な複数の異なる署名データを生成する。

- 次に、第2の手段が、前記第1の手段で生成した前記複数の署名データの各々について、当該署名データと前記データSとを含む識別データを生成し、複数の前記識別データを異なる複数の記録媒体にそれぞれ割当てて。
- 25

第10の発明のデータ処理方法は、記録媒体に割当てられた当該記録媒体を識

別する識別データの正当性を検証するデータ処理方法であって、前記識別データの管理元の公開鍵データを用いて前記識別データ内の署名データから第1のデータを生成し、当該第1のデータと前記識別データ内の第2のデータとを比較して前記識別データの正当性を検証する第1の工程と、前記第1の工程で前記識別データが正当であると検証した場合に、前記記録媒体から読み出した暗号データを、前記識別データ内の前記第2のデータを用いて復号する第2の工程とを有する。

第10の発明のデータ処理方法の作用は以下のようになる。

先ず、第1の工程において、前記識別データの管理元の公開鍵データを用いて前記識別データ内の署名データから第1のデータを生成し、当該第1のデータと前記識別データ内の第2のデータとを比較して前記識別データの正当性を検証する。

次に、第2の工程において、前記第1の工程で前記識別データが正当であると検証した場合に、前記記録媒体から読み出した暗号データを、前記識別データ内の前記第2のデータを用いて復号する。

上記各工程はデータ処理装置によって実行される。

第11の発明のプログラムは、記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置が実行するプログラムであって、

前記識別データの管理元の公開鍵データを用いて前記識別データ内の署名データから第1のデータを生成し、当該第1のデータと前記識別データ内の第2のデータとを比較して前記識別データの正当性を検証する第1の手順と、前記第1の手順で前記識別データが正当であると検証した場合に、前記記録媒体から読み出した暗号データを、前記識別データ内の前記第2のデータを用いて復号する第2の手順とを有する。

第12の発明のデータ処理装置は、記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置であって、前記識別データの管理元の公開鍵データを用いて前記識別データ内の署名データから第1のデー

タを生成し、当該第1のデータと前記識別データ内の第2のデータとを比較して前記識別データの正当性を検証する第1の手段と、前記第1の手段で前記識別データが正当であると検証した場合に、前記記録媒体から読み出した暗号データを、前記識別データ内の前記第2のデータを用いて復号する第2の手段とを有する。

5 第12の発明のデータ処理装置の作用は以下のようになる。

先ず、第1の手段が、前記識別データの管理元の公開鍵データを用いて前記識別データ内の署名データから第1のデータを生成する。

次に、前記第1の手段が、前記第1のデータと前記識別データ内の第2のデータとを比較して前記識別データの正当性を検証する。

10 次に、第2の手段が、前記第1の手段で前記識別データが正当であると検証した場合に、前記記録媒体から読み出した暗号データを、前記識別データ内の前記第2のデータを用いて復号する。

第13の発明のデータ処理方法は、公開されたデータ  $M$  を2つの素数の積とし、 $T$  を  $W$  ( $W \geq 2$ ) 個の異なる素数  $p(w)$  の積とし、 $w$  を  $1 \leq w \leq W$  の整数とし、 $K$  を巡回群  $Z * M$  の生成元とした場合に、 $W$  個の記録媒体  $STM(w)$  の各々に割当てる識別データ  $ID(w)$  を生成するデータ処理方法であって、 $(KT/p(w) \bmod M)$  を算出する第1の工程と、 $p(w)$  と前記第1の工程で算出した  $(KT/p(w) \bmod M)$  とを含む識別データ  $ID(w)$  を、記録媒体  $STM(w)$  に割当てる第2の工程とを有する。

20 第13の発明のデータ処理方法の作用は以下のようになる。

先ず、第1の工程において、 $(KT/p(w) \bmod M)$  を算出する。

次に、第2の工程において、 $p(w)$  と前記第1の工程で算出した  $(KT/p(w) \bmod M)$  とを含む識別データ  $ID(w)$  を、記録媒体  $STM(w)$  に割当てる。

25 上記各工程は、データ処理装置によって実行される。

第14の発明のプログラムは、公開されたデータ  $M$  を2つの素数の積とし、 $T$



を  $W$  ( $W \geq 2$ ) 個の異なる素数  $p(w)$  の積とし、 $w$  を  $1 \leq w \leq W$  の整数とし、 $K$  を巡回群  $Z * M$  の生成元とした場合に、 $W$  個の記録媒体  $STM(w)$  の各々に割当てる識別データ  $ID(w)$  を生成するデータ処理装置が実行するプログラムであって、 $(KT/p(w) \bmod M)$  を算出する第 1 の手順と、 $p(w)$  と前記

- 5 第 1 の手順で算出した  $(KT/p(w) \bmod M)$  とを含む識別データ  $ID(w)$  を、記録媒体  $STM(w)$  に割当てる第 2 の手順とを有する。

- 第 15 の発明のデータ処理装置は、公開されたデータ  $M$  を 2 つの素数の積とし、 $T$  を  $W$  ( $W \geq 2$ ) 個の異なる素数  $p(w)$  の積とし、 $w$  を  $1 \leq w \leq W$  の整数とし、 $K$  を巡回群  $Z * M$  の生成元とした場合に、 $W$  個の記録媒体  $STM(w)$  の各々に割当てる識別データ  $ID(w)$  を生成するデータ処理装置であって、 $(KT/p(w) \bmod M)$  を算出する第 1 の手段と、 $p(w)$  と前記第 1 の手段が算出した  $(KT/p(w) \bmod M)$  とを含む識別データ  $ID(w)$  を、記録媒体  $STM(w)$  に割当てる第 2 の手段とを有する。

第 15 の発明のデータ処理装置の作用は以下になる。

- 15 先ず、第 1 の手段が、 $(KT/p(w) \bmod M)$  を算出する。

次に、第 2 の手段が、 $p(w)$  と前記第 1 の手段が算出した  $(KT/p(w) \bmod M)$  とを含む識別データ  $ID(w)$  を、記録媒体  $STM(w)$  に割当てる。

- 第 16 の発明のデータ処理方法は、記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理方法であって、前記識別データに含まれるデータ  $p$  が素数であるか否かを検証する第 1 の工程と、前記第 1 の工程で前記データ  $p$  が素数であると検証された場合に、前記識別データに含まれるデータ  $IDKey$  と前記データ  $p$  と公開されているデータ  $M$  と用いて  $(IDKey p \bmod M)$  を算出する第 2 の工程と、前記第 2 の工程で算出した  $(IDKey p \bmod M)$  を基に得た復号鍵を用いて、前記記録媒体に記録された暗号データを復号する第 3 の工程とを有する。

第 16 の発明のデータ処理方法の作用は以下になる。

先ず、第1の工程において、前記識別データに含まれるデータ  $p$  が素数であるか否かを検証する。

次に、第2の工程において、前記第1の工程で前記データ  $p$  が素数であると検証された場合に、前記識別データに含まれるデータ  $IDKey$  と前記データ  $p$  と

5 公開されているデータ  $M$  と用いて  $(IDKey \cdot p \bmod M)$  を算出する。

次に、第3の工程において、前記第2の工程で算出した  $(IDKey \cdot p \bmod M)$  を基に得た復号鍵を用いて、前記記録媒体に記録された暗号データを復号する。

上記各工程は、データ処理装置によって実行される。

10 第17の発明のプログラムは、記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置が実行するプログラムであって、前記識別データに含まれるデータ  $p$  が素数であるか否かを検証する第1の手順と、前記第1の手順で前記データ  $p$  が素数であると検証された場合に、前記識別データに含まれるデータ  $IDKey$  と前記データ  $p$  と公開されているデータ  $M$  と用い  
15 て  $(IDKey \cdot p \bmod M)$  を算出する第2の手順と、前記第2の手順で算出した  $(IDKey \cdot p \bmod M)$  を基に得た復号鍵を用いて、前記記録媒体に記録された暗号データを復号する第3の手順とを有する。

第18の発明のデータ処理装置は、記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置であって、前記識別データ  
20 に含まれるデータ  $p$  が素数であるか否かを検証する第1の手段と、前記第1の手段が前記データ  $p$  が素数であると検証した場合に、前記識別データに含まれるデータ  $IDKey$  と前記データ  $p$  と公開されているデータ  $M$  と用いて  $(IDKey \cdot p \bmod M)$  を算出する第2の手段と、前記第2の手段が算出した  $(IDKey \cdot p \bmod M)$  を基に得た復号鍵を用いて、前記記録媒体に記録された暗号データ  
25 を復号する第3の手段とを有する。

第18の発明のデータ処理装置の作用は以下になる。

先ず、第1の手段が、前記識別データに含まれるデータ  $p$  が素数であるか否かを検証する。

次に、第2の手段が、前記第1の手段が前記データ  $p$  が素数であると検証した場合に、前記識別データに含まれるデータ  $IDKey$  と前記データ  $p$  と公開されているデータ  $M$  とを用いて  $(IDKey \cdot p \bmod M)$  を算出する。

次に、第3の手段が、前記第2の手段が算出した  $(IDKey \cdot p \bmod M)$  を基に得た復号鍵を用いて、前記記録媒体に記録された暗号データを復号する。

第19の発明のデータ処理方法は、素数  $q_1$  と  $q_2$  の積であり公開されたデータを  $M$  とし、 $w$  を  $1 \leq w \leq W$  の整数とし、 $W$  ( $W \geq 2$ ) 個の異なるデータを  $e(w)$  とし、 $e(w)$  を巡回群  $Z * M$  の生成元とし、 $e(w)$  と  $\lambda(M)$  は互いに素であり、 $\lambda(M)$  を  $(q_1 - 1)$  と  $(q_2 - 1)$  との最小公倍数とした場合に、 $W$  個の記録媒体  $STM(w)$  の各々に割当てて識別データ  $ID(w)$  を生成するデータ処理方法であって、巡回群  $Z * M$  の生成元であるデータ  $S$  と、 $\lambda(M)$  を法としたときの  $e(w)$  の逆数であるデータ  $d(w)$  と、上記データ  $M$  とを用いて、 $(S \cdot d(w) \bmod M)$  を算出する第1の工程と、前記  $e(w)$  と前記第1の工程で算出した  $(S \cdot d(w) \bmod M)$  とを含む識別データ  $ID(w)$  を、記録媒体  $STM(w)$  に割当てて第2の工程とを有する。

第19の発明のデータ処理方法の作用は以下のようなになる。

先ず、第1の工程において、巡回群  $Z * M$  の生成元であるデータ  $S$  と、 $\lambda(M)$  を法としたときの  $e(w)$  の逆数であるデータ  $d(w)$  と、上記データ  $M$  とを用いて、 $(S \cdot d(w) \bmod M)$  を算出する。

次に、第2の工程において、前記  $e(w)$  と前記第1の工程で算出した  $(S \cdot d(w) \bmod M)$  とを含む識別データ  $ID(w)$  を、記録媒体  $STM(w)$  に割当てて。

上記各工程は、データ処理装置によって実行される。

第20の発明のプログラムは、素数  $q_1$  と  $q_2$  の積であり公開されたデータを

Mとし、 $w$ を $1 \leq w \leq W$ の整数とし、 $W$  ( $W \geq 2$ ) 個の異なるデータを $e(w)$ とし、 $e(w)$ を巡回群 $Z * M$ の生成元とし、 $e(w)$ と $\lambda(M)$ は互いに素であり、 $\lambda(M)$ を $(q_1 - 1)$ と $(q_2 - 1)$ との最小公倍数とした場合に、 $W$  個の記録媒体 $S_{TM}(w)$ の各々に割当てて識別データ $ID(w)$ を生成するデータ処理装置が

5 実行するプログラムであって、巡回群 $Z * M$ の生成元であるデータ $S$ と、 $\lambda(M)$ を法としたときの $e(w)$ の逆数であるデータ $d(w)$ と、上記データ $M$ とを用いて、 $(S d(w) \bmod M)$ を算出する第1の手順と、前記 $e(w)$ と前記第1の手順で算出した $(S d(w) \bmod M)$ とを含む識別データ $ID(w)$ を、記録媒体 $S_{TM}(w)$ に割当てて第2の手順とを有する。

- 10 第21の発明のデータ処理装置は、素数 $q_1$ と $q_2$ の積であり公開されたデータを $M$ とし、 $w$ を $1 \leq w \leq W$ の整数とし、 $W$  ( $W \geq 2$ ) 個の異なるデータを $e(w)$ とし、 $e(w)$ を巡回群 $Z * M$ の生成元とし、 $e(w)$ と $\lambda(M)$ は互いに素であり、 $\lambda(M)$ を $(q_1 - 1)$ と $(q_2 - 1)$ との最小公倍数とした場合に、 $W$  個の記録媒体 $S_{TM}(w)$ の各々に割当てて識別データ $ID(w)$ を生成するデータ処理装置であって、巡回群 $Z * M$ の生成元であるデータ $S$ と、 $\lambda(M)$ を法としたときの $e(w)$ の逆数であるデータ $d(w)$ と、上記データ $M$ とを用いて、 $(S d(w) \bmod M)$ を算出する第1の手段と、前記 $e(w)$ と前記第1の手段が算出した $(S d(w) \bmod M)$ とを含む識別データ $ID(w)$ を、記録媒体 $S_{TM}(w)$ に割当てて第2の手段とを有する。

- 20 第21の発明のデータ処理装置の作用は以下になる。

まず、第1の手段が、巡回群 $Z * M$ の生成元であるデータ $S$ と、 $\lambda(M)$ を法としたときの $e(w)$ の逆数であるデータ $d(w)$ と、上記データ $M$ とを用いて、 $(S d(w) \bmod M)$ を算出する。

- 次に、第2の手段が、前記 $e(w)$ と前記第1の手段が算出した $(S d(w) \bmod M)$ とを含む識別データ $ID(w)$ を、記録媒体 $S_{TM}(w)$ に割当てて。
- 25

第22の発明のデータ処理方法は、記録媒体に割当てられた当該記録媒体を識

別する識別データの正当性を検証するデータ処理方法であって、前記識別データに含まれるデータ  $e$  およびデータ  $I$  と公開されているデータ  $M$  と用いて  $(Ie \bmod M)$  を算出する第1の工程と、前記第1の工程で算出した  $(Ie \bmod M)$  を復号鍵として用いて、前記記録媒体に記録された暗号データを復号する第2の工程とを有する。

第22の発明のデータ処理方法の作用は以下になる。

まず、第1の工程において、前記識別データに含まれるデータ  $e$  およびデータ  $I$  と公開されているデータ  $M$  と用いて  $(Ie \bmod M)$  を算出する。

次に、第2の工程において、前記第1の工程で算出した  $(Ie \bmod M)$  を復号鍵として用いて、前記記録媒体に記録された暗号データを復号する。

第23の発明のプログラムは、記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置が実行するプログラムであって、前記識別データに含まれるデータ  $e$  およびデータ  $I$  と公開されているデータ  $M$  と用いて  $(Ie \bmod M)$  を算出する第1の手順と、前記第1の手順で算出した  $(Ie \bmod M)$  を復号鍵として用いて、前記記録媒体に記録された暗号データを復号する第2の手順とを有する。

第24の発明のデータ処理装置は、記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置であって、前記識別データに含まれるデータ  $e$  およびデータ  $I$  と公開されているデータ  $M$  と用いて  $(Ie \bmod M)$  を算出する第1の手段と、前記第1の手が算出した  $(Ie \bmod M)$  を復号鍵として用いて、前記記録媒体に記録された暗号データを復号する第2の手段とを有する。

第24の発明のデータ処理装置の作用は以下になる。

まず、第1の手段が、前記識別データに含まれるデータ  $e$  およびデータ  $I$  と公開されているデータ  $M$  と用いて  $(Ie \bmod M)$  を算出する。

次に、第2の手段が、前記第1の手が算出した  $(Ie \bmod M)$  を復号鍵と

して用いて、前記記録媒体に記録された暗号データを復号する。

第25の発明の記録媒体は、データを記録する記録媒体であって、前記記録媒体の管理元の秘密鍵データを用いて生成され、前記管理元の公開鍵データを基に正当性が検証され、当該記録媒体を識別する識別データを記録している。

5 第26の発明の記録媒体は、データを記録する記録媒体であって、前記記録媒体の管理元の公開鍵データを用いて第1のデータを生成するために用いられる署名データと、前記第1のデータと比較して識別データの正当性を検証するために用いられる第2のデータとを含み前記記録媒体を識別する前記識別データを記録している。

10 第27の発明の記録媒体は、暗号データを記録する記録媒体であって、素数であるデータ  $p$  と、前記暗号データを復号するために用いられるコンテンツ鍵データである  $(IDKey_p \bmod M)$  を前記データ  $p$  と公開されているデータ  $M$  と共に算出するために用いられるデータ  $IDKey$  とを含み前記記録媒体を識別する識別データを記録している。

15 第28の発明の記録媒体は、暗号データを記録する記録媒体であって、前記暗号データを復号するために用いられるコンテンツ鍵データである  $(Ie \bmod M)$  を、公開されているデータ  $M$  と共に算出するために用いられるデータ  $e$  およびデータ  $I$  とを含み前記記録媒体を識別する識別データを記録している。

## 20 図面の簡単な説明

図1は、本発明の実施形態に係わるディスク型記録媒体に記録されるデータを説明するための図である。

図2は、本発明の実施形態に係わるコンテンツ提供システムの全体構成図である。

25 図3は、図2に示す管理装置の構成図である。

図4は、図3に示す管理装置によるディスクIDの生成処理を説明するための

フローチャートである。

図5は、図2に示すディスク製造装置の構成図である。

図6は、図5に示すディスク製造装置によるディスク製造手順を説明するためのフローチャートである。

- 5 図7は、図1に示すディスク型記録媒体に記録されるリボケーションリストDIRLのデータ構成を説明する図である。

図8は、MAC値生成処理例を示す図である。

図9は、各種キー、データの暗号化処理、配布処理について説明するツリー構成図である。

- 10 図10は、各種キー、データの配布に使用される有効化キーブロック(EKB)の例を示す図である。

図11は、コンテンツ鍵の有効化キーブロック(EKB)を使用した配布例と復号処理例を示す図である。

図12は、有効化キーブロック(EKB)のフォーマット例を示す図である。

- 15 図13は、有効化キーブロック(EKB)のタグの構成を説明する図である。

図14は、ツリー構成におけるカテゴリ分割を説明する図である。

図15は、ツリー構成におけるカテゴリ分割を説明する図である。

図16は、図2に示す再生装置の構成図である。

- 20 図17は、図16に示す再生装置の再生処理を説明するためのフローチャートである。

図18は、図17に示すステップST32のディスクIDの検証処理を説明するためのフローチャートである。

図19は、図17に示すステップST38の再生処理を説明するためのフローチャートである。

- 25 図20は、本発明の第2実施形態における管理装置のディスクIDの生成処理を説明するためのフローチャートである。

図 2 1 は、本発明の第 2 実施形態における再生装置による図 1 7 に示すステップ S T 3 2 のディスク I D の検証処理を説明するためのフローチャートである。

図 2 2 は、本発明の第 2 実施形態における再生装置による図 1 7 に示すステップ S T 3 8 の再生処理を説明するためのフローチャートである。

5 図 2 3 は、本発明の第 3 実施形態における管理装置のディスク I D の生成処理を説明するためのフローチャートである。

図 2 4 は、本発明の第 3 実施形態における再生装置による図 1 7 に示すステップ S T 3 2 のディスク I D の検証処理を説明するためのフローチャートである。

10 図 2 5 は、本発明の第 3 実施形態における再生装置による図 1 7 に示すステップ S T 3 8 の再生処理を説明するためのフローチャートである。

図 2 6 は、本発明の第 4 実施形態における管理装置のディスク I D の生成処理を説明するためのフローチャートである。

図 2 7 は、本発明の第 4 実施形態における再生装置による再生処理を説明するためのフローチャートである。

15

#### 発明を実施するための最良の形態

これより図面を参照して本発明の好適実施例について説明していく。

#### <第 1 実施形態>

当該実施形態は、第 1 ～第 6 および第 2 5 の発明に対応した実施形態である。

20 [ディスク型記録媒体 2]

図 1 は、本発明の実施形態に係わるディスク型記録媒体 2 (第 2 5 の発明の記録媒体) に記録されるデータを説明するための図である。

ディスク型記録媒体 2 は、C D (Compact Disc)、D V D (Digital Versatile Disk)、M D (Mini Disk) やその他のディスク型の記録媒体である。

25 ディスク型記録媒体 2 が第 2 5 の発明の記録媒体に対応している。なお、本発明の記録媒体は、ディスク型以外に、フラッシュメモリなどの半導体記録装置や



その他の記録媒体であってもよい。

図1に示すように、ディスク型記録媒体2には、ディスクIDと、暗号化コンテンツデータECONTと、暗号鍵情報EKBと、ディスクIDのリボケーションリストDIRLとが記録される。

- 5 ディスクIDは、ディスク型記録媒体2を識別するための識別データであり、消去や書き換えが困難であるようにディスク型記録媒体2に格納される。

ディスクIDが本発明の識別データに対応している。ディスクIDの生成方法については後述する。

- 10 なお、以下に説明する実施形態では、ディスク状の媒体をコンテンツ格納情報記録媒体の例として示しているので、その識別データをディスクIDとして説明する。

フラッシュメモリ等の各種の情報記録媒体を利用した場合にもディスクIDに対応する識別データが設定される。

- 15 暗号化コンテンツデータECONTは、暗号化されたコンテンツデータであり、暗号化コンテンツデータECONTを復号するためのコンテンツ鍵データは、例えば階層型鍵データ配信構成によって、正当なコンテンツ利用機器としての再生装置に提供されるデバイスノード鍵データ(DNK: Device Node Key)に基づいて、ディスク型記録媒体2に格納された暗号鍵情報である有効化鍵ブロック(EKB: Enabling Key Block)の復号処理等によって取得される。

- 20 階層型鍵データ配信構成によるデバイスノード鍵データDNKの提供、およびデバイスノード鍵データDNKに基づく有効化鍵ブロックEKBの復号処理による鍵取得処理の詳細については後述する。

- また、ディスクIDのリボケーションリスト(DIRL: Disc ID Revocation List)は、不正コピー等が行われたと認定されたディスク、例えば市場に不正な  
25 コピーコンテンツを格納したCD-Rが発見された場合に、その不正CD-RにコンテンツとともにコピーされたディスクIDを抽出し、リスト化したデータで

ある。リボケーションリストD I R Lの生成、管理、ディスク製造者に対するリスト情報提供は、特定の信頼される管理局（C A : Central Authority）が実行する。

〔システム構成〕

- 5 図2は、本発明の第1実施形態に係わるコンテンツ提供システム1の構成図である。

図2に示すように、コンテンツ提供システム1は、管理局C Aが使用する管理装置12と、コンテンツプロバイダが使用するコンテンツ提供装置13と、ディスク製造者が使用するディスク製造装置14と、ユーザが使用する再生装置15

10 とを有する。

ここで、管理装置12が第2および第3の発明のデータ処理装置に対応している。

また、再生装置15が第5および第6の発明のデータ処理装置に対応している。

- 15 なお、本実施形態では、再生装置15を例示するが、ディスク型記録媒体2に記録されたディスクIDの正当性を検証し、その結果を基に処理を行うものであれば、再生装置15の他に、例えば、ディスク型記録媒体2から読み出したコンテンツデータを記録または編集などを行うデータ処理装置を用いてもよい。

管理装置12が、前述したディスクIDとリボケーションリストD I R Lとを生成してディスク製造装置14に提供する。

- 20 また、コンテンツ提供装置13が、暗号化コンテンツE C O N Tと有効化鍵ブロックE K Bとをディスク製造装置14に提供する。

ディスク製造装置14は、管理装置12から受けたディスクIDおよびリボケーションリストD I R Lと、コンテンツ提供装置13から受けた暗号化コンテンツデータE C O N Tと有効化鍵ブロックE K Bとを記録したディスク型記録媒体

25 2を製造する。

ユーザは、ディスク型記録媒体2を例えば購入し、再生装置15にセットする。

再生装置 1 5 は、ディスク型記録媒体 2 に記録されたディスク ID が正当であると検証し、当該ディスク ID がリボケーションリスト D I R L 内に存在しないことを確認し、自らのデバイスノード鍵データ D N K に基づいて有効化鍵ブロック E K B から適切なコンテンツ鍵データを取得したことを条件に、暗号化コンテンツデータ E C O N T を復号し、続いて再生する。

以下、図 2 に示すコンテンツ提供システム 1 を構成する各装置について詳細に説明する。

#### 〔管理装置 1 2〕

図 3 は、図 2 に示す管理装置 1 2 の構成図である。

- 10 図 3 に示すように、管理装置 1 2 は、例えば、メインメモリ 2 2、セキュアメモリ 2 3、入出力インタフェース ( I / F ) 2 4、記録媒体インタフェース ( I / F ) 2 5、演算ユニット 2 6 およびコントローラ 2 7 を有し、これらがバス 2 1 を介して接続されている。

- 15 メインメモリ 2 2 は、演算ユニット 2 6 およびコントローラ 2 7 の処理に用いられる種々のデータのうち、セキュリティレベルが低いデータを記憶する。

セキュアメモリ 2 3 は、演算ユニット 2 6 およびコントローラ 2 7 の処理に用いられる種々のデータのうち、セキュリティレベルが高いデータを記憶する。

セキュアメモリ 2 3 は、例えば、ディスク ID の生成に用いられる管理局 C A の秘密鍵データなどを記憶する。

- 20 入出力インタフェース 2 4 は、例えば、図示しない操作手段あるいはネットワークなどに接続され、管理装置 1 2 が使用する種々のデータを入力する。

記録媒体インタフェース 2 5 は、コントローラ 2 7 の制御の基に生成されたディスク ID およびリボケーションリスト D I R L を記録媒体 2 9 a に書き込む。

記録媒体 2 9 a は、コンテンツ提供装置 1 3 に提供される。

- 25 また、記録媒体インタフェース 2 5 は、コントローラ 2 7 の制御の基に生成されたデバイスノード鍵データ D N K を記録媒体 2 9 b に書き込む。

記録媒体 29b は、再生装置 15、あるいは再生装置 15 の製造元に提供される。

演算ユニット 26 は、コントローラ 27 からの制御に基づいて、署名データを生成し、これを基にディスク ID を生成する。

5      また、演算ユニット 26 は、リボケーションリスト D I R L を生成する。

コントローラ 27 は、プログラム P R G 1（第 2 の発明のプログラム）を実行して管理装置 12 の処理を統括的に制御する。

本実施形態における管理装置 12 の機能（処理）は、コントローラ 27 によるプログラム P R G 1 の実行に応じて規定される。

10      管理装置 12 の機能（処理）の全部あるいは一部は、プログラム P R G 1 によって規定されてもよいし、ハードウェアによって実現されてもよい。

以下、図 3 に示す管理装置 12 によるディスク ID の生成動作を説明する。

図 4 は、図 3 に示す管理装置 12 によるディスク ID の生成動作を説明するためのフローチャートである。

15      図 4 において、ステップ S T 2 が第 1 の発明の第 1 の工程に対応し、ステップ S T 3 が第 1 の発明の第 2 の工程に対応している。

また、コントローラ 27 がステップ S T 2 を実行することで第 3 の発明の第 1 の手段が実現され、ステップ S T 3 を実行することで第 3 の発明の第 2 の手段が実現される。

20      ステップ S T 1 :

管理装置 12 のコントローラ 27 は、デジタル署名のための鍵データである管理局 C A の公開鍵データ（第 1 の発明の公開鍵データ）および秘密鍵データ（第 1 ～第 3 の発明の秘密鍵データ）、並びに署名生成および検証のためのパラメータを決定する。

25      コントローラ 27 は、上記公開鍵データおよび上記パラメータを公開する。

コントローラ 27 は、例えば、出力インタフェース 24 からネットワーク上に

上記公開鍵データおよび上記パラメータを送信して上記公開を行う。

ステップST1の処理は、管理装置12のセットアップ時に一度だけ行えばよい。

ステップST2:

- 5 管理装置12は、入出力インタフェース24を介して、コンテンツプロバイダから、コンテンツ（たとえば映画）のタイトルと、製造するディスク型記録媒体2の枚数 $W$  ( $W \geq 2$ )を入力し、これをメインメモリ22に格納する。

- 10 演算ユニット26は、任意のメッセージ $M$ （第1の発明の第2のデータ）と、乱数 $r(w)$ と、管理局CAの秘密鍵データとを用いて、 $W$ 個のデジタルの異なる署名データ $SIG(w)$ （第1～第3の発明の署名データ）を生成する。

当該署名データ $SIG(w)$ は、管理局CAの上記秘密鍵データに対応する公開鍵データを用いて、その改竄の有無、並びに正当性を確認可能な形態で生成される。

ここで、 $w = 1, 2, \dots, W$ であり、 $r(w)$ はそれぞれ個別の乱数である。

- 15 なお、演算ユニット26は、それぞれ個別の $W$ 個のメッセージ $M(w)$ （必ずしも個別の乱数でなくてもよい）を基に、署名データ $SIG(w)$ を生成してもよい。

- 20 演算ユニット26は、上記署名データ $SIG(w)$ の生成方法として、署名生成時に署名者が任意の乱数を使うことができる方法である、FIPS PUB 186-2で米国標準の署名方式となっているDSAや、その楕円曲線暗号版であるECDSAなどを用いている。DSA(Digital Signature Algorithm)はたとえば、岡本龍明、山本博資著、「現代暗号」、産業図書、1997のpp. 179-180に解説が記されており、ECDSAに関して<http://group.er.ieee.org/groups/1363/tradPK/index.html>から入手可能な仕様書にその詳細が記されている。

ステップST3:

コントローラ 27 は、ステップ ST1 で決定したメッセージ M あるいは M(w) とステップ ST2 で生成した署名データ SIG(w) とを用いて、(M, SIG(w)) の組もしくは (M(w), SIG(w)) の組を w 番目のディスク ID(w) として生成し、それをタイトルとともにディスク製造者にセキュアな状態で提供する。

具体的には、例えば、図 3 に示す記録媒体 29a にディスク ID(w) を記録してディスク製造者に提供する。

また、管理装置 12 は、リボークする情報記録媒体のディスク ID を示すリボケーションリスト DIRL を生成し、これもディスク製造者に提供する。

#### 10     〔ディスク製造装置 14〕

図 5 は、図 1 に示すディスク製造装置 14 の構成図である。

図 5 に示すように、ディスク製造装置 14 は、例えば、入出力インタフェース 32、暗号処理部 33、メモリ 34、コントローラ 35 および記録媒体インタフェース 36 を有し、これらがバス 31 を介して接続されている。

15     入出力インタフェース 32 は、外部から供給されるデジタル信号を受信し、バス 31 上に出力する。

入出力インタフェース 32 は、例えば、コンテンツ提供装置 13 からの暗号化コンテンツデータ ECONT および有効化鍵ブロック EKB を入力する。

また、入出力インタフェース 32 は、上記記録媒体 19a などを通じて管理装置 20     12 からディスク ID(w) およびリボケーションリスト DIRL などのデータを入力する。

なお、入出力インタフェース 32 は、製造するディスクの数に応じた数のディスク ID(w) を管理装置 12 から受ける。

また、入出力インタフェース 32 は、コンテンツ提供装置 13 から記録媒体などを通じて暗号化コンテンツデータ ECONT および有効化鍵ブロック EKB を 25     入力する。

暗号処理部 33 は、例えば、1 チップの L S I (Large Scale Integrated Circuit) で構成され、バス 31 を介して供給されるコンテンツとしてのデジタル信号を暗号化し、または復号し、バス 31 上に出力する構成を持つ。

なお、暗号処理部 33 は 1 チップ L S I に限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。

メモリ 34 は、コンテンツ提供装置 13 から受領した暗号化コンテンツデータ ECONT および有効化鍵ブロック EKB と、管理装置 12 から受けたディスク ID およびリボケーションリスト DIRL とを格納する。

コントローラ 35 は、ディスク製造装置 14 の処理を統括的に制御する。

10 記録媒体インタフェース 36 は、コントローラ 35 の制御の基に、種々のデータを書き込んだ図 1 に示すディスク型記録媒体 2 を製造する。

以下、図 5 に示すディスク製造装置 14 の動作例を説明する。

図 6 は、図 5 に示すディスク製造装置 14 の動作例を説明するためのフローチャートである。

15 ステップ ST11 :

ディスク製造装置 14 は、入出力インタフェース 32 を介して、上記記録媒体 19a を介して W 個のディスク ID (w) およびリボケーションリスト DIRL を管理装置 12 から入力してメモリ 34 に書き込む。

ステップ ST12 :

20 ディスク製造装置 14 は、入出力インタフェース 32 を介して、有効化鍵ブロック EKB をコンテンツ提供装置 13 から入力してメモリ 34 に書き込む。

ステップ ST13 :

ディスク製造装置 14 は、入出力インタフェース 32 を介して、暗号化コンテンツデータ ECONT をコンテンツ提供装置 13 から入力してメモリ 34 に書き込む。

25

ステップ ST14 :

ディスク製造装置 14 のコントローラ 35 は、リボケーションリスト D I R L、有効化鍵ブロック E K B および暗号化コンテンツデータ E C O N T をメモリ 34 から読み出し、これらのデータを情報記録媒体（ディスク）に書き込んでマスターディスクを製造する。

5      ステップ S T 1 5 :

コントローラ 35 は、ステップ S T 1 4 で製造したマスターディスクに基づくスタンプによるスタンプ処理により、複製としてのディスクを製造する。

ステップ S T 1 6 :

10      コントローラ 35 は、ステップ S T 1 5 で製造したディスクに、メモリ 34 から読み出したディスク I D (w) を書き込んでディスク型記録媒体 2 を製造する。

ステップ S T 1 7 :

コントローラ 35 は、W 枚のディスク型記録媒体 2 を製造したか否かを判断し、製造したと判断した場合には処理を終了し、そうでない場合にはステップ S T 1 5 の処理に戻る。

15      このように、ディスク製造装置 14 は、管理装置 12 から受けたディスク型記録媒体 2 の数 W に応じて、それぞれの製造ディスクに異なるディスク I D (w) を書き込む。

従って、市場に流通するディスク型記録媒体 2 にはそれぞれ異なるディスク I D (w) が設定されていることになり、同一のディスク I D (w) が記録された  
20      複数のディスク型記録媒体 2 が発見された場合は、不正なコピーが実行されているものと判断し、管理局 C A がリボケーションリスト D I R L にそのディスク I D (w) を書き込む更新処理を実行し、更新されたリストがディスク製造業者に提供され、新規ディスクには、そのリストが格納される。

ディスク型記録媒体 2 を購入したユーザが、再生装置 15 にディスク型記録媒  
25      体 2 をセットし、コンテンツ再生処理を実行する際には、再生装置 15 内のメモリに格納されたリボケーションリスト D I R L とのバージョン比較が実行され、



更新されたリストがメモリに格納される。従って、ユーザの再生装置 15 のメモリに格納されるリストは、随時更新される。

以下、管理装置 12 が製造するリボケーションリスト D I R L について説明する。

5 図 7 は、図 1 に示すリボケーションリスト D I R L を説明するための図である。

図 7 に示すように、リボケーションリスト D I R L は、当該リボケーションリスト D I R L が作成された時期に応じて値が増加するバージョン番号 5 1 と、無効に（リボーク）すべきディスク型記録媒体 2 のディスク I D （w）を羅列したリボークディスク I D リスト 5 2 と、バージョン番号 5 1 とリボークディスク I D リスト 5 2 に対する改竄検証値 5 3 としての認証子が含まれる。

改竄検証値 5 3 は、対象となるデータ、この場合はバージョン番号 5 1 とリボークディスク I D リスト 5 2 が改竄されているか否かを判別するために適用するデータであり、公開鍵暗号技術を用いたデジタル署名や、共通鍵暗号技術を用いたメッセージ認証コード（M A C : Message Authentication Code）が適用される。

15 改竄検証値 5 3 として公開鍵暗号技術を用いたデジタル署名を用いる際には、信頼できる機関、例えば上述の管理局 C A の署名検証鍵（公開鍵）を再生機が取得し、管理局 C A の署名生成鍵（秘密鍵）を用いて作られた署名を各再生機が取得した署名検証鍵（公開鍵）によって検証することで、バージョン番号 5 1 とリボークディスク I D リスト 5 2 が改竄されているか否かを判別する。

20 図 8 は、改竄検証値 5 3 としてメッセージ認証コード M A C を用いた際の M A C 生成、検証処理を説明するための図である。

メッセージ認証コード M A C は、データの改竄検証用のデータとして生成されるものであり、M A C 生成処理、検証処理態様には様々な態様が可能であるが、1 例として D E S 暗号処理構成を用いた M A C 値生成例を図 8 を基に説明する。

25 図 8 に示すように、対象となるメッセージ、この場合は、図 7 に示すバージョン番号 5 1 とリボークディスク I D リスト 5 2 を 8 バイト単位に分割し、（以下、

分割されたメッセージをM1、M2、・・・、MNとする)、まず、初期値 (Initial Value (IV)) とM1を排他的論理和する (その結果をI1とする)。

次に、I1をDES暗号化部に入れ、鍵 (以下、K1とする) を用いて暗号化する (出力をE1とする)。

- 5 続けて、E1およびM2を排他的論理和し、その出力I2をDES暗号化部へ入れ、鍵K1を用いて暗号化する (出力E2)。以下、これを繰り返し、全てのメッセージに対して暗号化処理を施す。最後に出てきたENがメッセージ認証符号MACとなる。

- 10 MAC値は、その生成元データが変更されると、異なる値となり、検証対象のデータ (メッセージ) に基づいて生成したMACと、記録されているMACとの比較を行い、一致していれば、検証対象のデータ (メッセージ) は変更、改竄がなされていないことが証明される。

- MAC生成における鍵K1としては、たとえば、階層型鍵データ配信構成によるデバイスノード鍵データDNKに基づく有効化鍵ブロック (EKB) の復号処理によって得られる鍵 (ルート鍵データ) を適用することが可能である。また、  
15 初期値IVとしては、予め定めた値を用いることが可能である。

[階層型鍵配信ツリー構成]

- 以下、ブロードキャストエンクリプション (Broadcast Encryption) 方式の一態様である階層型鍵配信ツリー構成に従った鍵提供処理、再生機としての再生装置  
20 管理構成について説明する。

図9の最下段に示すナンバ0～15がコンテンツ利用を行なうユーザデバイスである。本実施形態では、当該ユーザデバイスは、図2に示す再生装置15に対応している。

- 図4に示す階層ツリー (木) 構造の各葉 (リーフ : leaf) がそれぞれのデバイス  
25 に相当する。

各デバイス0～15は、製造時あるいは出荷時、あるいはその後において、図

9に示す階層ツリー（木）構造における自分のリーフからルートに至るまでのノードに割り当てられた鍵（ノード鍵データ）および各リーフのリーフ鍵データからなる鍵データセット（デバイスノード鍵データDNKをメモリに格納する。

図9の最下段に示すK0000～K1111が各デバイス0～15にそれぞれ割り当てられたリーフ鍵データであり、最上段のKR（ルート鍵データ）から、最下段から2番目の節（ノード）に記載された鍵データ：KR～K1111をノード鍵データとする。

図9に示すツリー構成において、例えばデバイス0はリーフ鍵データK0000と、ノード鍵データ：K000、K00、K0、KRを所有する。デバイス5はK0101、K010、K01、K0、KRを所有する。デバイス15は、K1111、K111、K11、K1、KRを所有する。

なお、図9のツリーにはデバイスが0～15の16個のみ記載され、ツリー構造も4段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

また、図9のツリー構造に含まれる各デバイスには、様々な記録媒体、例えば、デバイス埋め込み型あるいはデバイスに着脱自在に構成されたDVD、CD、MD、フラッシュメモリ等を使用する様々なタイプのデバイスが含まれている。

さらに、様々なアプリケーションサービスが共存可能である。このような異なるデバイス、異なるアプリケーションの共存構成の上に図9に示すコンテンツあるいは鍵配布構成である階層ツリー構造が適用される。

これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図9の点線で囲んだ部分、すなわちデバイス0、1、2、3を同一の記録媒体を用いる1つのグループとして設定する。

例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダからネットワークまたはCD等の

情報記録媒体に格納して提供したり、各デバイス共通に使用するコンテンツ鍵データを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。

- 5      コンテンツサーバ、ライセンスサーバ、あるいはショップサーバ等、各デバイスとのデータ送受信を行なうエンティティは、図9の点線で囲んだ部分、すなわちデバイス0, 1, 2, 3を1つのグループとして一括してデータを送付する処理を実行可能となる。このようなグループは、図9のツリー中に複数存在する。

- 10      なお、ノード鍵データ、リーフ鍵データは、ある1つの鍵管理センター機能を持つ管理システムによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等のメッセージデータ配信手段によってグループごとに管理する構成としてもよい。これらのノード鍵データ、リーフ鍵データは例えば鍵データの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センター機能を持つ管理システム、プロバイダ、決済機関等が実行  
15      可能である。

このツリー構造において、図9から明らかなように、1つのグループに含まれる3つのデバイス0, 1, 2, 3はデバイスノード鍵データDNKとして共通の鍵データK00、K0、KRを含むデバイスノード鍵データDNKを保有する。

- 20      このノード鍵データ共有構成を利用することにより、例えば共通の鍵データをデバイス0, 1, 2, 3のみに提供することが可能となる。たとえば、共通に保有するノード鍵データK00は、デバイス0, 1, 2, 3に共通する保有鍵データとなる。

- 25      また、新たな鍵データKnewをノード鍵データK00で暗号化した値Enc(K00, Knew)を、ネットワークを介してあるいは記録媒体に格納してデバイス0, 1, 2, 3に配布すれば、デバイス0, 1, 2, 3のみが、それぞれのデバイスにおいて保有する共有ノード鍵データK00を用いて暗号Enc(K

00, Knew) を解いて新たな鍵データ Knew を得ることが可能となる。なお、Enc (Ka, Kb) は Kb を Ka によって暗号化したデータであることを示す。

また、ある時点 t において、デバイス 3 の所有する鍵 : K0011, K001, K00, K0, KR が攻撃者 (ハッカー) により解析されて露呈したことが発覚した場合、それ以降、システム (デバイス 0, 1, 2, 3 のグループ) で送受信されるデータを守るために、デバイス 3 をシステムから切り離す必要がある。

そのためには、ノード鍵データ : K001, K00, K0, KR をそれぞれ新たな鍵 K(t)001, K(t)00, K(t)0, K(t)R に更新し、デバイス 0, 1, 2 にその更新鍵データを伝える必要がある。ここで、K(t)aaa は、鍵 Kaaa の世代 (Generation) : t の更新鍵データであることを示す。

更新鍵データの配布処理について説明する。鍵データの更新は、例えば、図 10 (A) に示す有効化鍵ブロック EKB によって構成されるテーブルをたとえばネットワーク、あるいは記録媒体に格納してデバイス 0, 1, 2 に供給することによって実行される。

なお、有効化鍵ブロック EKB は、図 9 に示すようなツリー構造を構成する各リーフに対応するデバイスに新たに更新された鍵データを配布するための暗号化鍵データによって構成される。有効化鍵ブロック EKB は、鍵データ更新ブロック (KRB : Key Renewal Block) と呼ばれることもある。

図 10 (A) に示す有効化鍵ブロック EKB には、ノード鍵データの更新の必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。

図 10 の例は、図 9 に示すツリー構造中のデバイス 0, 1, 2 において、世代 t の更新ノード鍵データを配布することを目的として形成されたブロックデータである。

図 9 から明らかなように、デバイス 0, デバイス 1 は、更新ノード鍵データと

して $K(t)00$ 、 $K(t)0$ 、 $K(t)R$ が必要であり、デバイス2は、更新ノード鍵データとして $K(t)001$ 、 $K(t)00$ 、 $K(t)0$ 、 $K(t)R$ が必要である。

図10(A)のEKBに示されるようにEKBには複数の暗号化鍵データが含まれる。最下段の暗号化鍵データは、 $Enc(K0010, K(t)001)$ である。これはデバイス2の持つリーフ鍵データ $K0010$ によって暗号化された更新ノード鍵データ $K(t)001$ であり、デバイス2は、自身の持つリーフ鍵データによってこの暗号化鍵データを復号し、 $K(t)001$ を得ることができる。

10 また、復号により得た $K(t)001$ を用いて、図10(A)の下から2段目の暗号化鍵データ $Enc(K(t)001, K(t)00)$ を復号可能となり、更新ノード鍵データ $K(t)00$ を得ることができる。

以下順次、図10(A)の上から2段目の暗号化鍵データ $Enc(K(t)00, K(t)0)$ を復号し、更新ノード鍵データ $K(t)0$ 、図10(A)の上  
15 から1段目の暗号化鍵データ $Enc(K(t)0, K(t)R)$ を復号し $K(t)R$ を得る。一方、デバイス $K0000$ 、 $K0001$ は、ノード鍵データ $K000$ は更新する対象に含まれておらず、更新ノード鍵データとして必要なのは、 $K(t)00$ 、 $K(t)0$ 、 $K(t)R$ である。

デバイス $K0000$ 、 $K0001$ は、図10(A)の上から3段目の暗号化鍵  
20 データ $Enc(K000, K(t)00)$ を復号し $K(t)00$ 、を取得し、以下、図10(A)の上から2段目の暗号化鍵データ $Enc(K(t)00, K(t)0)$ を復号し、更新ノード鍵データ $K(t)0$ 、図10(A)の上から1段目の暗号化鍵データ $Enc(K(t)0, K(t)R)$ を復号し $K(t)R$ を得る。  
このようにして、デバイス0, 1, 2は更新した鍵 $K(t)R$ を得ることができ  
25 る。

なお、図10(A)のインデックスは、復号鍵データとして使用するノード鍵

データ、リーフ鍵データの絶対番地を示す。

図9に示すツリー構造の上位段のノード鍵データ： $K(t)O$ ,  $K(t)R$ の更新が不要であり、ノード鍵データ $KOO$ のみの更新処理が必要である場合には、図10(B)の有効化鍵ブロックEKBを用いることで、更新ノード鍵データ $K(t)OO$ をデバイス0, 1, 2に配布することができる。

図10(B)に示すEKBは、例えば特定のグループにおいて共有する新たなコンテンツ鍵データを配布する場合に利用可能である。

具体例として、図9に点線で示すグループ内のデバイス0, 1, 2, 3がある記録媒体を用いており、新たな共通のコンテンツ鍵データ $K(t)con$ が必要であるとする。

このとき、デバイス0, 1, 2, 3の共通のノード鍵データ $KOO$ を更新した $K(t)OO$ を用いて新たな共通の更新コンテンツ鍵データ： $K(t)con$ を暗号化したデータ $Enc(K(t)OO, K(t)con)$ を図10(B)に示すEKBとともに配布する。この配布により、デバイス4など、その他のグループの機器においては復号されないデータとしての配布が可能となる。

すなわち、デバイス0, 1, 2はEKBを処理して得た $K(t)OO$ を用いて上記暗号文を復号すれば、 $t$ 時点での鍵データ、例えばコンテンツの暗号化復号化に適用するコンテンツ鍵データ $K(t)con$ を得ることが可能になる。

図11に、 $t$ 時点での鍵データ、例えばコンテンツの暗号化復号化に適用するコンテンツ鍵データ $K(t)con$ をEKBの処理によって取得する処理例を示す。

EKBには、 $K(t)OO$ を用いてコンテンツ鍵データ $K(t)con$ を暗号化したデータ $Enc(K(t)OO, K(t)con)$ と図10(B)に示すデータとが格納されているとする。ここでは、デバイス0の処理例を示す。

図11に示すように、デバイス0は、記録媒体に格納されている世代： $t$ 時点のEKBと自分があらかじめ格納しているノード鍵データ $KOOO$ を用いて上述

したと同様のEKB処理により、ノード鍵データK(t) 00を生成する。

さらに、復号した更新ノード鍵データK(t) 00を用いて暗号化データEnc(K(t) 00, K(t) con)を復号して更新コンテンツ鍵データK(t) conを取得する。さらに、デバイスは、後にそれを使用するために自分だけが持つリーフ鍵データK0000で暗号化して格納してもよい。

また、別の例として、ツリー構造のノード鍵データの更新は不必要で、時点tでのコンテンツ鍵データK(t) conのみを必要な機器が得られればよい、という場合もある。この場合、下記のような方式とすることができる。

いま、図11の例と同様に、デバイス0、1、2にのみコンテンツ鍵データK(t) conを送りたいとする。このとき、EKBは、  
バージョン (Version): t

インデックス 暗号化鍵データ

000 Enc(K000, K(t) con)

0010 Enc(K0010, K(t) con)

15 となる。

デバイス0、1はK000を用いて、またデバイス2はK0010を用いて上記EKBのうちの1つの暗号文を復号することによりコンテンツ鍵データを得ることができる。このようにすることにより、ノード鍵データの更新は行えないものの、必要な機器にコンテンツ鍵データを与える方法をより効率よく(すなわち、EKBに含まれる暗号文数を減らしてEKBのサイズを小さくするとともに、管理センタでの暗号化およびデバイスでの復号処理の回数を減らせる)することができる。

図12に有効化鍵ブロックEKBのフォーマット例を示す。バージョン61は、有効化鍵ブロックEKBのバージョンを示す識別子である。なお、バージョンは最新のEKBを識別する機能とコンテンツとの対応関係を示す機能を持つ。デバイスは、有効化鍵ブロックEKBの配布先のデバイスに対する階層ツリーの階層数



を示す。データポインタ 6 3 は、有効化鍵ブロック E K B 中のデータ部の位置を示すポインタであり、タグポインタ 6 4 はタグ部の位置、署名ポインタ 6 5 は署名の位置を示すポインタである。

データ部 6 6 は、例えば更新するノード鍵データを暗号化したデータを格納する。例えば図 5 に示すような更新されたノード鍵データに関する各暗号化鍵データ等を格納する。

タグ部 6 7 は、データ部に格納された暗号化されたノード鍵データ、リーフ鍵データの位置関係を示すタグである。このタグの付与ルールを図 1 3 を用いて説明する。

- 10 図 1 3 では、データとして先に図 1 0 (A) で説明した有効化鍵ブロック E K B を送付する例を示している。

この時のデータは、図 1 3 の表 (b) に示すようになる。このときの暗号化鍵データに含まれるトップノードのアドレスをトップノードアドレスとする。この場合は、ルート鍵データの更新鍵データ  $K(t)R$  が含まれているので、トップ  
15 ノードアドレスは  $KR$  となる。

- このとき、例えば最上段のデータ  $Enc(K(t)0, K(t)R)$  は、図 1 3 の (a) に示す階層ツリーに示す位置にある。ここで、次のデータは、 $Enc(K(t)00, K(t)0)$  であり、ツリー上では前のデータの左下の位置にある。データがある場合は、タグが 0、ない場合は 1 が設定される。タグは {左  
20 (L) タグ, 右 (R) タグ} として設定される。最上段のデータ  $Enc(K(t)0, K(t)R)$  の左にはデータがあるので、L タグ = 0、右にはデータがないので、R タグ = 1 となる。以下、すべてのデータにタグが設定され、図 1 3 (c) に示すデータ列、およびタグ列が構成される。

- タグは、データ  $Enc(Kxxx, Kyyy)$  がツリー構造のどこに位置して  
25 いるのかを示すために設定されるものである。データ部に格納される鍵データ  $Enc(Kxxx, Kyyy)...$  は、単純に暗号化された鍵データの羅列データに

過ぎないので、上述したタグによってデータとして格納された暗号化鍵データのツリー上の位置を判別可能としたものである。上述したタグを用いずに、先の図 10 で説明した構成のように暗号化データに対応させたノード・インデックスを用いて、例えば、

- 5      0 : Enc (K (t) 0, K (t) root)
- 00 : Enc (K (t) 00, K (t) 0)
- 000 : Enc (K ((t) 000, K (T) 00)

... のようなデータ構成とすることも可能であるが、このようなインデックスを用いた構成とすると冗長なデータとなりデータ量が増大し、ネットワークを介する配信等においては好ましくない。

これに対し、上述したタグを鍵データ位置を示す索引データとして用いることにより、少ないデータ量で鍵データ位置の判別が可能となる。

- 図 12 に戻って、EKB フォーマットについてさらに説明する。署名 (Signature) 68 は、有効化鍵ブロック EKB を発行した例えば鍵管理センター機能を持つ管理システム、コンテンツサーバ、ライセンスサーバ、あるいはショップサーバ等が実行する電子署名である。EKB を受領したデバイスは署名検証によって正当な有効化鍵ブロック EKB 発行者が発行した有効化鍵ブロック EKB であることを確認する。

- ノード鍵データ等を定義している階層ツリー構造を各デバイスのカテゴリ毎に分類して効率的な鍵データ更新処理、暗号化鍵データ配信、データ配信を実行する構成について、以下説明する。

図 14 は、階層ツリー構造のカテゴリの分類の一例を説明するための図である。

- 図 14 において、階層ツリー構造の最上段には、ルート鍵データ K r o o t 71 が設定され、以下の中間段にはノード鍵データ 72 が設定され、最下段には、リーフ鍵データ 73 が設定される。各デバイスは個々のリーフ鍵データと、リーフ鍵データからルート鍵データに至る一連のノード鍵データ、ルート鍵データを

保有する。

ここで、一例として最上段から第M段目のあるノードをカテゴリノード74として設定する。すなわち第M段目のノードの各々を特定カテゴリのデバイス設定ノードとする。第M段の1つのノードを頂点として以下、M+1段以下のノード、

- 5 リーフは、そのカテゴリに含まれるデバイスに関するノードおよびリーフとする。

例えば図14の第M段目の1つのノード75にはカテゴリAが設定され、このノード以下に連なるノード、リーフはカテゴリAに区分され、様々なデバイスを含むカテゴリA専用のノードまたはリーフとして設定される。すなわち、ノード75以下を、カテゴリAとして区分されるデバイスの関連ノード、およびリーフ

- 10 の集合として定義する。

さらに、M段から数段分下位の段をサブカテゴリノード76として設定することができる。

例えば図に示すようにカテゴリAノード75の2段下のノードに、カテゴリAに含まれるサブカテゴリAaノードとして、[再生専用器]のノードを設定する。

- 15 さらに、サブカテゴリAaノードである再生専用器のノード76以下に、再生専用器のカテゴリに含まれる音楽再生機能付き電話のノード77が設定され、さらにその下位に、音楽再生機能付き電話のカテゴリに含まれる[PHS]ノード78と[携帯電話]ノード79を設定することができる。

- さらに、カテゴリ、サブカテゴリは、デバイスの種類、メーカー、コンテンツ  
20 プロバイダ、決済機関等が独自に管理するノード、すなわち処理単位、管轄単位、あるいは提供サービス単位等、任意の単位で設定可能である。例えば1つのカテゴリノードをゲーム機器メーカーの販売するゲーム機器XYZ専用の頂点ノードとして設定すれば、メーカーの販売するゲーム機器XYZにその頂点ノード以下の下段のノード鍵データ、リーフ鍵データを格納して販売することが可能となり、  
25 その後、暗号化コンテンツデータの配信、あるいは各種鍵データの配信、更新処理を、その頂点ノード鍵データ以下のノード鍵データ、リーフ鍵データによって

構成される有効化鍵ブロック E K B を生成して配信し、頂点ノード以下のデバイスに対してのみ利用可能なデータが配信可能となる。

また、コンテンツプロバイダの管理するノードをカテゴリノードとした場合には、コンテンツプロバイダが提供するコンテンツを格納した C D、M D、D V D 等の情報記録媒体またはネット配信コンテンツを利用する機器をカテゴリノード以下に設定して、その機器に対してその頂点ノード以下の下段のノード鍵データ、リーフ鍵データを提供することが可能となる。

このように、1つのノードを頂点として、以下のノードをその頂点ノードに定義されたカテゴリ、あるいはサブカテゴリの関連ノードとして設定する構成とすることにより、カテゴリ段、あるいはサブカテゴリ段の1つの頂点ノードを管理するメーカー、コンテンツプロバイダ等がそのノードを頂点とする有効化鍵ブロック (E K B) を独自に生成して、頂点ノード以下に属するデバイスに配信する構成が可能となり、頂点ノードに属さない他のカテゴリのノードに属するデバイスには全く影響を及ぼさずに鍵データ更新を実行することができる。

例えば、図 1 5 に示されるように、ツリー構成のシステムで、鍵データ管理が行われる。

図 1 5 の例では、8 + 2 4 + 3 2 段のノードがツリー構造とされ、ルートノードから下位の 8 段までの各ノードにカテゴリが対応される。ここにおけるカテゴリとは、例えばフラッシュメモリなどの半導体メモリを使用する機器のカテゴリ、デジタル放送を受信する機器のカテゴリといったカテゴリを意味する。

そして、このカテゴリノードのうちの1つのノードに、ライセンスを管理するシステムとして本システム (T システムと称する) が対応する。

すなわち、この T システムのノードよりさらに下の階層の 2 4 段のノードに対応する鍵データが、ショップサーバ、ライセンスサーバ等の管理エンティティとしてのサービスプロバイダ、あるいはサービスプロバイダが提供するサービスに適用される。

この例の場合、これにより、224（約16メガ）のサービスプロバイダあるいはサービスを規定することができる。さらに、最も下側の32段の階層により、232（約4ギガ）のユーザ（あるいはユーザデバイス）を規定することができる。

最下段の32段のノードからTシステムのノードまでのパス上の各ノードに対応する鍵データが、DNKを構成し、最下段のリーフに対応するIDがリーフIDとされる。

例えば、コンテンツを暗号化したコンテンツ鍵データは更新されたルート鍵データKR'によって暗号化され、上位の階層の更新ノード鍵データは、その直近の下位の階層の更新ノード鍵データを用いて暗号化され、EKB内に配置される。

10 EKBにおける末端から1つ上の段の更新ノード鍵データはEKBの末端のノード鍵データあるいはリーフ鍵データによって暗号化され、EKB内に配置される。

ユーザデバイスは、サービスデータに記述されているDNKのいずれかの鍵データを用いて、コンテンツデータとともに配布されるEKB内に記述されている直近の上位の階層の更新ノード鍵データを復号し、復号して得た鍵データを用いて、EKB内に記述されているさらにその上の階層の更新ノード鍵データを復号する。以上の処理を順次行うことで、ユーザデバイスは、更新ルート鍵データKR'を得ることができる。

上述したように、ツリーのカテゴリ分類により、1つのノードを頂点として、以下のノードをその頂点ノードに定義されたカテゴリ、あるいはサブカテゴリの  
20 関連ノードとして設定した構成が可能となり、カテゴリ段、あるいはサブカテゴリ段の1つの頂点ノードを管理するメーカー、サービスプロバイダ等がそのノードを頂点とする有効化鍵ブロックEKBを独自に生成して、頂点ノード以下に属するデバイスに配信する構成が実現される。

〔再生装置15〕

25 図16は、図2に示す再生装置15の構成図である。

図16に示すように、再生装置15は、例えば、入出力インタフェース81、

MPEG (Moving Picture Experts Group)等の各種符号化データの生成および復号を実行するコーデック82、A/D・D/Aコンバータ84を備えた入出力インタフェース83、暗号処理部85、ROM (Read Only Memory) 86、コントローラ87、メモリ88、並びにディスク型記録媒体2にアクセスするための記録媒体インタフェース89を有し、これらがバス80によって相互に接続されている。

入出力インタフェース81は、ネットワーク等、外部から供給されるデジタル信号を受信し、バス80上に出力するとともに、バス80上のデジタル信号を受信し、外部に出力する。

- 10     コーデック82は、バス80を介して供給される例えばMPEG符号化されたデータをデコードし、入出力インタフェース83に出力するとともに、入出力インタフェース83から供給されるデジタル信号をエンコードしてバス80上に出力する。

入出力インタフェース83は、コンバータ84を内蔵している。

- 15     入出力インタフェース83は、外部から供給されるアナログ信号を受信し、コンバータ84でA/D (Analog Digital)変換することで、デジタル信号として、コーデック82に出力するとともに、コーデック82からのデジタル信号をコンバータ84でD/A (Digital Analog)変換することで、アナログ信号として、外部に出力する。

- 20     暗号処理部85は、例えば、1チップのLSIで構成され、バス80を介して供給される例えばコンテンツ等のデジタル信号を暗号化し、または復号し、バス80上に出力する構成を持つ。

なお、暗号処理部85は1チップLSIに限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。

- 25     ROM86は、例えば、再生装置ごとに固有の、あるいは複数の再生装置のグループごとに固有のデバイス鍵データであるリーフ鍵データと、複数の再生装置、

あるいは複数のグループに共有のデバイス鍵データであるノード鍵データを記憶している。

コントローラ 87 は、メモリ 88 に記憶されたプログラム PRG 3（第 5 の発明のプログラム）を実行することで、再生装置 15 の処理を統括して制御する。

- 5     すなわち、再生装置 15 の機能（処理）は、プログラム PRG 3 によって規定される。なお、再生装置 15 の機能の全部あるいは一部を、ハードウェアによって実現してもよい。

メモリ 88 は、上述したリボケーションリスト D I R L をディスク型記録媒体 2 から読み取りセキュアな状態で格納する。

- 10     例えば再生装置 15 に設定された I D に基づく暗号化を施してメモリに格納するなどにより耐タンパ性を保持したデータとして格納することが好ましい。このようにリボケーションリスト D I R L は外部から消されたり、内容を改ざんされたり、古いバージョンのリストに入れ替えられることを容易に実行されないように格納する。

- 15     記録媒体インタフェース 89 は、ディスク型記録媒体 2 にアクセスするために用いられる。

以下、図 16 に示す再生装置 15 の動作例を説明する。

- 図 17 は図 16 に示す再生装置 15 の全体動作例を説明するためのフローチャート、図 18 は図 17 に示すステップ S T 3 2 のディスク I D の検証処理を説明するためのフローチャート、図 19 は図 17 に示すステップ S T 3 8 のコンテンツ再生を説明するためのフローチャートである。
- 20

ステップ S T 3 1 :

再生装置 15 は、所定のアクセス位置にディスク型記録媒体 2 がセットされると、記録媒体インタフェース 89 を介して、ディスク型記録媒体 2 からディスク

- 25     I D を読み出し、これをメモリ 88 に格納する。

ステップ S T 3 2 :

再生装置 15 のコントローラ 87 は、ステップ S T 3 1 でメモリ 88 に格納したディスク I D を読み出してその改竄の有無および正当性を検証する。

当該検証については、後に詳細に説明する。

ステップ S T 3 3 :

- 5     コントローラ 87 は、ステップ S T 3 2 で上記ディスク I D が正当であると検証するとステップ S T 3 5 の処理に進み、そうでない場合にはステップ S T 3 4 に進む。

ステップ S T 3 4 :

- 10    コントローラ 87 は、ディスク型記録媒体 2 に記録されている暗号化コンテンツデータ E C O N T の復号および再生を停止（禁止）する。

ステップ S T 3 5 :

コントローラ 87 は、記録媒体インタフェース 89 を介して、ディスク型記録媒体 2 からリボケーションリスト D I R L を読み出す。

- 15    そして、コントローラ 87 は、当該読み出したリボケーションリスト D I R L の改竄検証値として公開鍵暗号技術を用いたデジタル署名がなされている場合は、署名検証鍵（公開鍵）によって検証する。また、改竄検証値としてメッセージ認証コード M A C が付与されている場合は、先に図 8 を参照して説明した M A C 検証処理が実行される。

- 20    そして、コントローラ 87 は、リボケーションリスト D I R L に改竄がないと判定されたことを条件に、当該リボケーションリスト D I R L のバージョンと、メモリ 88 に既に格納されているリボケーションリスト D I R L とのバージョン比較を実行する。

- 25    コントローラ 87 は、当該読み出したリボケーションリスト D I R L のバージョンがメモリ 88 に既に格納されているリボケーションリスト D I R L より新しい場合は、当該読み出したリボケーションリスト D I R L によって、メモリ 88 内のリボケーションリスト D I R L を更新する。



ステップST36:

コントローラ87は、ステップST31で読み出したディスクIDがリボケーションリストDIRL内に存在するか否かを判断し、存在すると判断するとステップST38に進み、そうでない場合にはステップST37に進む。

5     ステップST37:

コントローラ87は、ディスク型記録媒体2に記録されている暗号化コンテンツデータECONTの復号および再生を停止（禁止）する。

ステップST38:

10    コントローラ87は、ディスク型記録媒体2に記録されている暗号化コンテンツデータECONTを読み出し、これを復号して再生する。

ステップST38の処理については、後に詳細に説明する。

以下、図17に示すディスクIDの検証(ST32)について詳細に説明する。

図18は、図17に示すステップST32を説明するためのフローチャートである。

15    図18の処理が、第4の発明の工程に対応し、ステップST42が第1の工程に対応し、ステップST43～ST46が第2の工程に対応している。

また、図18の処理をコントローラ87が行うことで、第6の発明の手段が実現される。

ステップST41:

20    再生装置15のコントローラ87は、図17に示すステップST31で読み出したディスクID(w)内の署名データSIG(w)（第4～第6の発明の署名データ）を取り出す。

ステップST42:

25    コントローラ87は、メモリ88から読み出した管理装置12（管理局CA）の公開鍵データ（第4～第6の発明の公開鍵データ）および公開されたパラメータを基に、ステップST41で読み出した署名データSIG(w)からメッセー

ジM (w)' (第4の発明の第1のデータ) を生成する。

ステップST43:

コントローラ87は、ディスクID (w) 内のメッセージM (w) あるいはM (第4の発明の第2のデータ) と、ステップST42で生成したメッセージM (w)' とを比較する。

ステップST44:

コントローラ87は、ステップST43の比較で一致していると判定するとステップST45に進み、そうでない場合にはステップST46に進む。

ステップST45:

10     コントローラ87は、ステップST41で取り出したディスクID (w) が正当であると判定する。

ステップST46:

コントローラ87は、ステップST41で取り出したディスクID (w) が不正であると判定する。

15     以下、図17に示すステップST38の再生処理について説明する。

図19は、図17に示すステップST38の再生処理を説明するためのフローチャートである。

ステップST51:

20     再生装置15は、記録媒体インタフェース89を介して、ディスク型記録媒体2から暗号鍵情報、すなわち有効化鍵ブロックEKBを読み出す。

ステップST52:

25     コントローラ87は、図11を用いて前述したように、階層型鍵データ配信構成によって予め再生装置に提供されているデバイスノード鍵データDNKに基づいて有効化鍵ブロックEKBの復号処理を実行して、コンテンツ鍵データを取得する。

ステップST53:

コントローラ 87 は、記録媒体インタフェース 89 を介して、ディスク型記録媒体 2 から暗号化コンテンツデータ ECONT を読み出す。

ステップ ST54 :

5     コントローラ 87 は、ステップ ST52 で取得したコンテンツ鍵データを用いて、ステップ ST53 で読み出した暗号化コンテンツデータ ECONT を復号する。

ステップ ST55 :

10    コントローラ 87 は、ディスク型記録媒体 2 に記録されている全ての暗号化コンテンツデータ ECONT を復号したと判断すると、処理を終了し、そうでない場合にはステップ ST53 に戻る。

以上説明したように、コンテンツ提供システム 1 では、ディスク型記録媒体 2 に記録するディスク ID を、管理装置 12 において、管理装置 12 の秘密鍵データを基に署名データとして生成する。

15    また、再生装置 15 において、ディスク型記録媒体 2 から読み出したディスク ID を、管理装置 12 の公開鍵データを用いて検証する。

そのため、ディスク型記録媒体 2 に記録されてるディスク ID が改竄されたり、不正者によって生成された場合に、そのことを再生装置 15 などが容易に検出できる。

20    その結果、不正に複製されたディスク型記録媒体 2 の流通を効果的に抑制することが可能になり、コンテンツ提供者の利益を保護できる。

上述したように、第 1 実施形態では、ディスク ID は任意の値ではなく、信頼できる機関である管理局 CA の管理装置 12 が生成し、署名したものを利用した。

25    また、上述した第 1 実施形態では、コンテンツデータを暗号化して暗号化コンテンツデータ ECONT を得るために利用したコンテンツ鍵データは、ディスク ID とは独立して生成されている。

以下に示す実施形態では、コンテンツ鍵データをディスク ID から導出する場合

合を例示する。

これにより、不正者が、任意のディスクIDを用いて海賊版ディスクを無制限に製造する効果をさらに高めることができる。

＜第2実施形態＞

- 5 第2実施形態は、第7～第12および第26の発明に対応した実施形態である。

本実施形態のコンテンツ提供システムは、図4に示す管理装置12によるディスクIDの生成処理、図18に示すディスクIDの検証処理、図19に再生処理におけるコンテンツ復号データの取得処理を除いて、第1実施形態のコンテンツ提供システム1と同じである。

- 10 本実施形態では、ディスクIDはディスクIDからタイトルごとに共通のメッセージSを導出できるように生成され、このメッセージSをコンテンツ鍵データとして用いる。

以下、本実施形態における管理装置12aのディスクID生成方法を説明する。

- 15 図20は、本実施形態のコンテンツ提供システムにおいて管理装置12aが行うディスクIDの生成方法を説明するためのフローチャートである。

図20に示す各処理は、コントローラ27がプログラムPRG1aを実行することによって実現され、この場合にプログラムPRG1aが第8の発明に対応する。

- 20 また、コントローラ27が図20に示す各ステップを実行することで、第9の発明の第1の手段および第2の手段が実現される。この場合に、管理装置12aが第8および第9の発明のデータ処理装置に対応している。

なお、図20に示す処理の全部または一部は、コントローラ27がプログラムPRG1aを実行する形態ではなく、同じ機能を実現する回路などのハードウェアによって実現してもよい。

- 25 ステップST101：

管理装置12aのコントローラ27は、デジタル署名のための鍵データ（管理

局CAの公開鍵データおよび秘密鍵データ)、並びに署名生成および検証のためのパラメータを決定する。

コントローラ27は、上記公開鍵データおよび上記パラメータを公開する。

当該公開は、例えば、コントローラ27が、入出力インタフェース24を介し

5 てネットワークを介して送信を行って実現する。

ステップST101の処理は、管理装置12のセットアップ時に一度だけ行えばよい。

ステップST102:

管理装置12は、入出力インタフェース24を介して、コンテンツプロバイダ  
10 から、コンテンツ(たとえば映画)のタイトルと、製造するディスクの枚数 $W$  ( $W \geq 2$ )を入力し、これをメインメモリ22に格納する。

演算ユニット26は、コンテンツデータのタイトルに対してメッセージ $S$ (第7～第9の発明のデータ $S$ )を決定する。

当該メッセージ $S$ が後述する、ディスクIDから導出される値となり、コンテ  
15 ンツ鍵データとして用いられる。

ステップST103:

演算ユニット26は、ステップST102で決定したメッセージ $S$ と、乱数 $r$   
( $w$ )と、上記パラメータとを用いて、 $W$ 個のデジタルの異なる署名データ $SIG(w)$ を生成する。

20 ここで、 $w=1, 2, \dots, W$ であり、 $r(w)$ はそれぞれ個別の乱数である。

ステップST104:

コントローラ27は、 $w$ 番目のディスクID( $w$ )として、( $S, SIG(w)$ )の組をタイトルとともにディスク製造者に提供する。

ディスク製造者のディスク製造装置14は、図6を用いて前述した手順で、上  
25 記ディスクID( $w$ )を記録したディスク型記録媒体2a(第26の発明の記録媒体)を製造する。

また、ディスク製造装置 14 は、ステップ S T 1 0 2 で決定したメッセージ S を、コンテンツ鍵データとしてコンテンツデータを暗号化した暗号化コンテンツデータ E C O N T をディスク型記録媒体 2 a に記録する。

以下、本実施形態における再生装置 15 a の動作例を説明する。

- 5      本実施形態の再生装置 15 a は、図 17 に示すステップ S T 3 2 およびステップ S T 3 8 の処理のみが第 1 実施形態の場合と異なる。

図 21 は、本実施形態における再生装置 15 a によるディスク I D の検証を説明するためのフローチャートである。

- 10      図 21 に示す処理が第 10 の発明の第 1 の工程に対応し、図 22 に示す処理が第 10 の発明の第 2 の工程に対応している。

また、コントローラ 87 が図 21 に示す処理を実行することで第 12 の発明の第 1 の手段が実現され、図 22 の処理を実行することで第 12 の発明の第 2 の手段が実現される。

- 15      また、以下に示す処理は、再生装置 15 b のコントローラ 87 がプログラム P R G 3 c (第 17 の発明のプログラム) を実行して実現される。

ステップ S T 1 1 1 :

再生装置 15 a のコントローラ 87 は、図 17 に示すステップ S T 3 1 で上述したディスク型記録媒体 2 a から読み出したディスク I D (w) 内の署名データ S I G (w) を取り出す。

- 20      ステップ S T 1 1 2 :

コントローラ 87 は、メモリ 88 から読み出した管理装置 12 (管理局 C A) の公開鍵データと公開されたパラメータとを基に、ステップ S T 1 1 1 で取り出した署名データ S I G (w) からメッセージ S' (第 10 ~ 第 12 の発明の第 1 のデータ) を生成する。

- 25      ステップ S T 1 1 3 :

コントローラ 87 は、ディスク I D (w) 内のメッセージ S (第 10 ~ 第 12

の発明の第2のデータ)と、ステップST112で生成したメッセージS'とを比較する。

ステップST114:

コントローラ87は、ステップST113の比較で一致していると判定すると

- 5 ステップST115に進み、そうでない場合にはステップST116に進む。

ステップST115:

コントローラ87は、ステップST111で取り出したディスクID(w)が正当であると判定する。

ステップST116:

- 10 コントローラ87は、ステップST111で取り出したディスクID(w)が不正であると判定する。

図22は、本実施形態における図17に示すステップST38の再生処理を説明するためのフローチャートである。

- 本実施形態において、ステップST51が無く、ステップST52の代わりに  
15 ステップST52aを行うこと以外は、図19を用いて第1実施形態で説明したものと同一である。

ステップST52a:

再生装置15aのコントローラ87は、図21の検証でディスクIDの正当性が認められたことを条件に、ディスクID(w)内のメッセージSと再生装置1

- 20 5aが取得した図9を用いて説明したルート鍵データとを基にコンテンツ鍵データ(復号鍵)を生成する。コントローラ87は、例えば、ルート鍵データと、メッセージSとの排他的論理和をコンテンツ鍵データとする。

本実施形態のコンテンツ提供システムによっても、第1実施形態のコンテンツ提供システム1と同様の効果が得られる。

## 25 <第3実施形態>

第3実施形態は、第13～第18および第27の発明に対応した実施形態であ

る。

本実施形態のコンテンツ提供システムは、図4に示す管理装置12によるディスクIDの生成処理、図18に示すディスクIDの検証処理、図19に再生処理におけるコンテンツ復号データの取得処理を除いて、第1実施形態のコンテンツ提供システム1と同じである。

本実施形態では、ディスクIDはディスクIDからタイトルごとに共通のメッセージSを導出できるように生成され、このメッセージSをコンテンツ鍵データとして用いる。

以下、本実施形態における管理装置12bのディスクID生成方法を説明する。

10 図23は、本実施形態のコンテンツ提供システムにおいて管理装置12bが行うディスクIDの生成方法を説明するためのフローチャートである。

図23に示す各処理は、管理装置12bのコントローラ27がプログラムPRG1bを実行することによって実現され、この場合にプログラムPRG1bが第14の発明に対応する。

15 また、コントローラ27が図23に示す各ステップを実行することで、第15の発明の第1の手段および第2の手段が実現される。この場合に、管理装置12bが第14および第15の発明のデータ処理装置に対応している。

20 なお、図23に示す処理の全部または一部は、コントローラ27がプログラムPRG1bを実行する形態ではなく、同じ機能を実現する回路などのハードウェアによって実現してもよい。

ステップST201:

管理装置12bのコントローラ27が、RSA暗号に用いるのに安全とされる程度に大きな素数 $q_1$ 、 $q_2$ を選択する。

ステップST202:

25 コントローラ27が、ステップST201で選択した素数 $q_1$ 、 $q_2$ の積であるデータMを公開する。



ステップST201, ST202の処理はシステムのセットアップ時に一度だけ行えばよい。

ステップST203:

5 コントローラ27が、各タイトルに対して、 $K \in Z * M$  ( $K$ は巡回群 $Z * M$ の生成元)を満たすデータ $K$ をランダムに選択する。

ここで、例えば、 $X \in Z * M$ は、 $X$ が、 $1 \sim X-1$ の整数 $x$ のなかで $x$ を法として逆元を持つ集合の要素であることを示す。

ステップST204:

10 コントローラ27が、コンテンツ製作者から、コンテンツのタイトルと製造するディスク型記録媒体2bの予定最大生産枚数 $W$ を受け取る。

ステップST205:

コントローラ27が、ステップST204の枚数 $W$ に対応した数だけ、素数 $p(w)$  ( $w=1, 2 \dots W$ )を定める。例えば、 $w$ 番目の奇素数を $p(w)$ と定めてもよい。

15 ステップST206:

コントローラ27が、そのタイトルに対応して、ディスクIDから導出される値をとして、データ $S (=KT \bmod M)$ を決定する。

但し、下記式(1)が成り立つ。

$$20 \quad T = \prod_{w=1}^W P_w \quad \dots (1)$$

ステップST207:

コントローラ27が、 $(KT/p(w) \bmod M)$ を演算して、その結果であるデータIDkey( $w$ )を得る。

25 ステップST208:

コントローラ27は、 $w$ 番目のディスクID( $w$ )として、ステップST20

5で決定した素数 $p(w)$ と、ステップST207で得たデータIDkey( $w$ )との組( $p(w)$ , IDkey( $w$ ))をディスクIDとしてタイトルとともにディスク製造者に提供する。

ディスク製造者のディスク製造装置14は、図6を用いて前述した手順で、上記ディスクID( $w$ )を記録したディスク型記録媒体2b(第27の発明の記録媒体)を製造する。

また、ディスク製造装置14は、上述したステップST206で決定したデータ $S(=KT \bmod M)$ をコンテンツ鍵データとしてコンテンツデータを暗号化して暗号化コンテンツデータECONTを生成し、これをディスク型記録媒体2bに記録する。

以下、本実施形態における再生装置15bの動作例を説明する。

本実施形態の再生装置15bは、図17に示すステップST32およびステップST38の処理のみが第1実施形態の場合と異なる。

図24は、本実施形態における再生装置15bによるディスクIDの検証を説明するためのフローチャートである。

図24に示す処理が第16の発明の第1の工程に対応している。

また、コントローラ87が図24に示す処理を実行することで第18の発明の第1の手段が実現される。

また、以下に示す処理は、再生装置15bのコントローラ87がプログラムPRG3b(第17の発明のプログラム)を実行して実現される。

ステップST211:

再生装置15bのコントローラ87は、図17に示すステップST31で上述したディスク型記録媒体2aから読み出したディスクID( $w$ )内のデータ $p(w)$ を取り出す。

ステップST212:

コントローラ87は、ステップST211で取り出したデータ $p(w)$ が素数

か否かを判断する

コントローラ 87 は、データ  $p(w)$  が素数であると判断するとステップ ST 213 に進み、そうでない場合にはステップ ST 214 に進む。

ステップ ST 213 :

- 5     コントローラ 87 は、ステップ ST 211 で取り出したディスク ID ( $w$ ) が正当であると判定する。

ステップ ST 214 :

コントローラ 87 は、ステップ ST 211 で取り出したディスク ID ( $w$ ) が不正であると判定する。

- 10    図 25 は、本実施形態における図 17 に示すステップ ST 38 の再生処理を説明するためのフローチャートである。

図 25 に示すステップ ST 221 が第 16 の発明の第 2 の工程に対応し、ステップ ST 224 が第 16 の発明の第 3 の工程に対応する。

- 15    また、コントローラ 87 がステップ ST 221 を実行することで第 18 の発明の第 1 の手段が実現され、ステップ ST 224 を実行することで第 18 の発明の第 2 の手段が実現される。

ステップ ST 221 :

- 20    再生装置 15b のコントローラ 87 は、記録媒体インタフェース 89 を介して、ディスク型記録媒体 2 から読み出したデータ  $p$ ,  $IDKey$  および公開されているデータ  $M$  を基に、 $(IDkey \cdot p \bmod M)$  を算出し、その結果をデータ  $S'$  とする。

ステップ ST 222 :

- 25    コントローラ 87 は、ステップ ST 221 で算出したデータ  $S'$  と、再生装置 15b が取得した図 9 を用いて説明したルート鍵データとを基にコンテンツ鍵データ (復号鍵) を生成する。コントローラ 87 は、例えば、ルート鍵データと、データ  $S'$  との排他的論理和をコンテンツ鍵データとする。

ステップST223:

コントローラ87は、記録媒体インタフェース89を介して、ディスク型記録媒体2bから暗号化コンテンツデータECONTを読み出す。

ステップST224:

- 5     コントローラ87は、ステップST222のコンテンツ鍵データを用いて、ステップST223で読み出した暗号化コンテンツデータECONTを復号する。

ステップST225:

- 10    コントローラ87は、ディスク型記録媒体2bに記録されている全ての暗号化コンテンツデータECONTを復号したと判断すると、処理を終了し、そうでない場合にはステップST223に戻る。

本実施形態のコンテンツ提供システムによっても、第1実施形態のコンテンツ提供システム1と同様の効果が得られる。

#### <第4実施形態>

- 15    第4実施形態は、第19～第24および第28の発明に対応した実施形態である。

本実施形態のコンテンツ提供システムは、図4に示す管理装置12によるディスクIDの生成処理、図18に示すディスクIDの検証処理、図19に再生処理におけるコンテンツ復号データの取得処理を除いて、第1実施形態のコンテンツ提供システム1と同じである。

- 20    以下、本実施形態における管理装置12cのディスクID生成方法を説明する。

図26は、本実施形態のコンテンツ提供システムにおいて管理装置12cが行うディスクIDの生成方法を説明するためのフローチャートである。

- 25    図26に示す各処理は、コントローラ27がプログラムPRG1cを実行することによって実現され、この場合にプログラムPRG1cが第20の発明に対応する。

また、コントローラ27が図26に示す各ステップを実行することで、第21

の発明の第 1 の手段および第 2 の手段が実現される。この場合に、管理装置 1 2 c が第 2 0 および第 2 1 の発明のデータ処理装置に対応している。

なお、図 2 6 に示す処理の全部または一部は、コントローラ 2 7 がプログラム P R G 1 c を実行する形態ではなく、同じ機能を実現する回路などのハードウェアによって実現してもよい。

ステップ S T 3 0 1 :

管理装置 1 2 c のコントローラ 2 7 が、R S A 暗号に用いるのに安全とされる程度に大きな素数  $q_1$ ,  $q_2$  を選択する。

ステップ S T 3 0 2 :

- 10     コントローラ 2 7 が、ステップ S T 3 0 1 で選択した素数  $q_1$ ,  $q_2$  の積であるデータ M を公開する。

ステップ S T 3 0 1, S T 3 0 2 の処理はシステムのセットアップ時に一度だけ行えばよい。

ステップ S T 3 0 3 :

- 15     コントローラ 2 7 が、各タイトルに対して、 $S \in Z^* M$  ( $S$  は巡回群  $Z^* M$  の生成元) を満たすデータ  $S$  をランダムに選択する。当該データ  $S$  がディスク I D から導出される値となる。

ステップ S T 3 0 4 :

- 20     コントローラ 2 7 が、コンテンツ製作者から、コンテンツのタイトルと製造するディスク型記録媒体 2 b 予定最大生産枚数  $W$  を受け取る。

ステップ S T 3 0 5 :

コントローラ 2 7 が、 $e(w) \in Z^* M$  ( $e(w)$  は巡回群  $Z^* M$  の生成元) を満たす互いに異なるデータ  $e(w)$  を選択する。

- 25     ここで、 $e(w)$  と  $\lambda(M)$  とは互いに素、すなわち、 $e(w)$  と  $\lambda(M)$  の最大公約数が 1 となる。なお、 $\lambda(M)$  は素数  $(q_1 - 1)$  と  $(q_2 - 1)$  との最少公倍数である。

ステップST306:

コントローラ27が、 $(Sd(w) \bmod M)$ を演算して、その結果であるデータI(w)を得る。

ここで、 $d(w)$ は、上記 $\lambda(M)$ を法としたときの上記 $e(w)$ の逆数である。すなわち、 $d(w) = e(w)^{-1} \bmod \lambda(M)$ となる。

ステップST307:

コントローラ27は、 $w$ 番目のディスクID(w)として、ステップST305で決定したデータ $e(w)$ と、ステップST306で得たデータI(w)との組 $(e(w), I(w))$ をディスクID(w)としてタイトルとともにディスク製造者に提供する。

ディスク製造者のディスク製造装置14は、図6を用いて前述した手順で、上記ディスクID(w)を記録したディスク型記録媒体2c(第28の発明の記録媒体)を製造する。

また、ディスク製造装置14は、上述したステップST303で選択したデータSをコンテンツ鍵データとしてコンテンツデータを暗号化して暗号化コンテンツデータECONTを生成し、これをディスク型記録媒体2cに記録する。

以下、本実施形態における再生装置15cの動作例を説明する。

図27は、再生装置15cの動作例を説明するための図である。

図27に示すステップST312が第22の発明の第1の工程に対応し、ステップST316が第22の発明の第2の工程に対応する。

また、コントローラ87がステップST312を実行することで第24の発明の第1の手段が実現され、ステップST316を実行することで第24の発明の第2の手段が実現される。

また、図27に示す各ステップは、再生装置15cのコントローラ87が、プログラムPRG3c(第23の発明のプログラム)を実行することで実現される。

ステップST311:

再生装置 15 c は、所定のアクセス位置にディスク型記録媒体 2 c がセットされると、記録媒体インタフェース 89 を介して、ディスク型記録媒体 2 c からディスク ID を読み出し、これをメモリ 88 に格納する。

ステップ ST 312 :

- 5 再生装置 15 c のコントローラ 87 は、メモリ 88 に記録したディスク ID 内のデータ  $e(w)$  と  $I(w)$  とを用いて、 $I(w)e(w) \bmod M$  を算出し、その結果をデータ  $S'$  とする。

ステップ ST 313 :

- 10 コントローラ 87 は、記録媒体インタフェース 89 を介して、ディスク型記録媒体 2 c からリボケーションリスト DIRL を読み出す。

- そして、コントローラ 87 は、当該読み出したリボケーションリスト DIRL の改竄検証値として公開鍵暗号技術を用いたデジタル署名がなされている場合は、署名検証鍵（公開鍵）によって検証する。また、改竄検証値としてメッセージ認証コード MAC が付与されている場合は、先に図 8 を参照して説明した MAC 検  
15 証処理が実行される。

そして、コントローラ 87 は、リボケーションリスト DIRL に改竄がないと判定されたことを条件に、当該リボケーションリスト DIRL のバージョンと、メモリ 88 に既に格納されているリボケーションリスト DIRL とのバージョン比較を実行する。

- 20 コントローラ 87 は、当該読み出したリボケーションリスト DIRL のバージョンがメモリ 88 に既に格納されているリボケーションリスト DIRL より新しい場合は、当該読み出したリボケーションリスト DIRL によって、メモリ 88 内のリボケーションリスト DIRL を更新する。

ステップ ST 314 :

- 25 コントローラ 87 は、ステップ ST 311 で読み出したディスク ID がリボケーションリスト DIRL 内に存在するか否かを判断し、存在すると判断するとス

テップST315に進み、そうでない場合にはステップST316に進む。

ステップST315：

コントローラ87は、ディスク型記録媒体2cに記録されている暗号化コンテンツデータECONTの再生を停止（禁止）する。

5      ステップST316：

コントローラ87は、ディスク型記録媒体2cに記録されている暗号化コンテンツデータECONTを読み出し、ステップST312で生成したデータS'を基に取得したコンテンツ鍵データを用いて、暗号化コンテンツデータECONTを復号し、続いて再生する。

10      コントローラ87は、例えば、ルート鍵データと、データS'との排他的論理和をコンテンツ鍵データとする。

本実施形態のコンテンツ提供システムによっても、第1実施形態のコンテンツ提供システム1と同様の効果が得られる。

15      本発明によれば、識別データを基に記録媒体を管理する場合に、その識別データを不正に生成並びに改竄することが困難な形態で生成できるデータ処理方法、そのプログラムおよびその装置を提供することができるという第1の効果が得られる。

20      また、本発明によれば、上記第1の効果をj得るデータ処理方法、そのプログラムおよびその装置によって生成された識別データを適切に検証できるデータ処理方法、そのプログラムおよびその装置を提供することができるという第2の効果が得られる。

また、本発明によれば、上記第1の効果をj得るデータ処理方法、そのプログラムおよびその装置によって生成された識別データを記録した記録媒体を提供できるという第3の効果が得られる。

25

産業上の利用可能性



本発明は、記録媒体を識別する識別データに係わる処理を行うデータ処理システムに利用可能である。

## 請 求 の 範 囲

1. 記録媒体を識別する識別データを生成するデータ処理方法であって、  
前記識別データの管理元の秘密鍵データを用いて、複数の異なる署名デー

5 タを生成する第1の工程と、

前記第1の工程で生成した前記複数の署名データを、前記識別データとして異なる複数の記録媒体にそれぞれ割当て第2の工程と

を有するデータ処理方法。

2. 前記第1の工程において、複数の異なる第1のデータの各々について、  
10 当該第1のデータと、前記秘密鍵データと、所定の第2のデータとを用いて、前記秘密鍵データに対応する公開鍵データを基に前記第2のデータを生成可能な前記複数の署名データを生成し、

前記第2の工程において、前記第1の工程で生成した前記複数の署名データの各々について、当該署名データと前記第2のデータとを含む前記識別データ

15 を生成し、当該識別データを前記記録媒体に割り当てる

請求項1に記載のデータ処理方法。

3. 記録媒体を識別する識別データを生成するデータ処理装置が実行するプログラムであって、

前記識別データの管理元の秘密鍵データを用いて、複数の異なる署名デー

20 タを生成する第1の手順と、

前記第1の手順で生成した前記複数の署名データを、前記識別データとして異なる複数の記録媒体にそれぞれ割当て第2の手順と

を有するプログラム。

4. 記録媒体を識別する識別データを生成するデータ処理装置であって、

25 前記識別データの管理元の秘密鍵データを用いて、複数の異なる署名データを生成する第1の手段と、

前記第 1 の手段で生成した前記複数の署名データを、前記識別データとして異なる複数の記録媒体にそれぞれ割当てて第 2 の手段と

を有するデータ処理装置。

5. 記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理方法であって、

前記識別データの管理元の公開鍵データを用いて、前記識別データの正当性を検証する工程

を有するデータ処理方法。

6. 前記工程は、

10 前記識別データに含まれる前記署名データから、前記公開鍵データを用いて第 1 のデータを生成する第 1 の工程と、

前記識別データに含まれる第 2 のデータと、前記第 1 の工程で生成した前記第 1 のデータとを比較し、当該比較の結果を基に、前記識別データの正当性を検証する第 2 の工程と

15 を有する請求項 5 に記載のデータ処理方法。

7. 記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置が実行するプログラムであって、

前記識別データの管理元の公開鍵データを用いて、前記識別データの正当性を検証する手順

20 を有するプログラム。

8. 記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置であって、

前記識別データの管理元の公開鍵データを用いて、前記識別データの正当性を検証する手段

25 を有するデータ処理装置。

9. 記録媒体を識別する識別データを生成するデータ処理方法であって、

前記識別データの管理元の秘密鍵データとデータ S とを用いて、前記管理元の公開鍵データを基に前記データ S を復号可能な複数の異なる署名データを生成する第 1 の工程と、

前記第 1 の工程で生成した前記複数の署名データの各々について、当該署名データと前記データ S とを含む識別データを生成し、複数の前記識別データを異なる複数の記録媒体にそれぞれ割当てる第 2 の工程と

を有するデータ処理方法。

10. 前記データ S を暗号化鍵として暗号化した暗号データと、前記識別データとを前記記録媒体に書き込む第 3 の工程

10 をさらに有する請求項 9 に記載のデータ処理方法。

11. 記録媒体を識別する識別データを生成するデータ処理装置が実行するプログラムであって、

前記識別データの管理元の秘密鍵データとデータ S とを用いて、前記管理元の公開鍵データを基に前記データ S を復号可能な複数の異なる署名データを生成する第 1 の手順と、

前記第 1 の手順で生成した前記複数の署名データの各々について、当該署名データと前記データ S とを含む識別データを生成し、複数の前記識別データを異なる複数の記録媒体にそれぞれ割当てる第 2 の手順と

を有するプログラム。

20 12. 記録媒体を識別する識別データを生成するデータ処理装置であって、

前記識別データの管理元の秘密鍵データとデータ S とを用いて、前記管理元の公開鍵データを基に前記データ S を復号可能な複数の異なる署名データを生成する第 1 の手段と、

25 前記第 1 の手段で生成した前記複数の署名データの各々について、当該署名データと前記データ S とを含む識別データを生成し、複数の前記識別データを

異なる複数の記録媒体にそれぞれ割当てて第 2 の手段と

を有するデータ処理装置。

1 3. 記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理方法であって、

- 5 前記識別データの管理元の公開鍵データを用いて前記識別データ内の署名データから第 1 のデータを生成し、当該第 1 のデータと前記識別データ内の第 2 のデータとを比較して前記識別データの正当性を検証する第 1 の工程と、

- 前記第 1 の工程で前記識別データが正当であると検証した場合に、前記記録媒体から読み出した暗号データを、前記識別データ内の前記第 2 のデータを用いて復号する第 2 の工程と

を有するデータ処理方法。

1 4. 記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置が実行するプログラムであって、

- 15 前記識別データの管理元の公開鍵データを用いて前記識別データ内の署名データから第 1 のデータを生成し、当該第 1 のデータと前記識別データ内の第 2 のデータとを比較して前記識別データの正当性を検証する第 1 の手順と、

前記第 1 の手順で前記識別データが正当であると検証した場合に、前記記録媒体から読み出した暗号データを、前記識別データ内の前記第 2 のデータを用いて復号する第 2 の手順と

- 20 を有するプログラム。

1 5. 記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置であって、

- 前記識別データの管理元の公開鍵データを用いて前記識別データ内の署名データから第 1 のデータを生成し、当該第 1 のデータと前記識別データ内の第 2 のデータとを比較して前記識別データの正当性を検証する第 1 の手段と、

前記第 1 の手段で前記識別データが正当であると検証した場合に、前記記

録媒体から読み出した暗号データを、前記識別データ内の前記第2のデータを用いて復号する第2の手段と

を有するデータ処理装置。

16. 公開されたデータ  $M$  を2つの素数の積とし、 $T$  を  $W$  ( $W \geq 2$ ) 個の異なる素数  $p(w)$  の積とし、 $w$  を  $1 \leq w \leq W$  の整数とし、 $K$  を巡回群  $Z * M$  の生成元とした場合に、 $W$  個の記録媒体  $STM(w)$  の各々に割当てる識別データ  $ID(w)$  を生成するデータ処理方法であって、

$(KT/p(w) \bmod M)$  を算出する第1の工程と、

- 10  $p(w)$  と前記第1の工程で算出した  $(KT/p(w) \bmod M)$  とを含む識別データ  $ID(w)$  を、記録媒体  $STM(w)$  に割当てる第2の工程とを有するデータ処理方法。

17.  $(KT \bmod M)$  を暗号化鍵として暗号化した暗号データと、前記識別データ  $ID(w)$  とを前記記録媒体  $STM(w)$  に書き込む第3の工程をさらに有する請求項16に記載のデータ処理方法。

- 15 18. 公開されたデータ  $M$  を2つの素数の積とし、 $T$  を  $W$  ( $W \geq 2$ ) 個の異なる素数  $p(w)$  の積とし、 $w$  を  $1 \leq w \leq W$  の整数とし、 $K$  を巡回群  $Z * M$  の生成元とした場合に、 $W$  個の記録媒体  $STM(w)$  の各々に割当てる識別データ  $ID(w)$  を生成するデータ処理装置が実行するプログラムであって、

$(KT/p(w) \bmod M)$  を算出する第1の手順と、

- 20  $p(w)$  と前記第1の手順で算出した  $(KT/p(w) \bmod M)$  とを含む識別データ  $ID(w)$  を、記録媒体  $STM(w)$  に割当てる第2の手順とを有するプログラム。

19. 公開されたデータ  $M$  を2つの素数の積とし、 $T$  を  $W$  ( $W \geq 2$ ) 個の異なる素数  $p(w)$  の積とし、 $w$  を  $1 \leq w \leq W$  の整数とし、 $K$  を巡回群  $Z * M$  の生成元とした場合に、 $W$  個の記録媒体  $STM(w)$  の各々に割当てる識別データ  $ID(w)$  を生成するデータ処理装置であって、
- 25

( $KT/p(w) \bmod M$ ) を算出する第1の手段と、

$p(w)$  と前記第1の手段が算出した ( $KT/p(w) \bmod M$ ) とを含む識別データ  $ID(w)$  を、記録媒体  $STM(w)$  に割当てて第2の手段とを有するデータ処理装置。

- 5            20. 記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理方法であって、

前記識別データに含まれるデータ  $p$  が素数であるか否かを検証する第1の工程と、

- 10           前記第1の工程で前記データ  $p$  が素数であると検証された場合に、前記識別データに含まれるデータ  $IDKey$  と前記データ  $p$  と公開されているデータ  $M$  とを用いて ( $IDKey p \bmod M$ ) を算出する第2の工程と、

前記第2の工程で算出した ( $IDKey p \bmod M$ ) を基に得た復号鍵を用いて、前記記録媒体に記録された暗号データを復号する第3の工程とを有するデータ処理方法。

- 15           21. 記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置が実行するプログラムであって、

前記識別データに含まれるデータ  $p$  が素数であるか否かを検証する第1の手順と、

- 20           前記第1の手順で前記データ  $p$  が素数であると検証された場合に、前記識別データに含まれるデータ  $IDKey$  と前記データ  $p$  と公開されているデータ  $M$  とを用いて ( $IDKey p \bmod M$ ) を算出する第2の手順と、

前記第2の手順で算出した ( $IDKey p \bmod M$ ) を基に得た復号鍵を用いて、前記記録媒体に記録された暗号データを復号する第3の手順とを有するプログラム。

- 25           22. 記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置であって、

前記識別データに含まれるデータ  $p$  が素数であるか否かを検証する第 1 の手段と、

前記第 1 の手段が前記データ  $p$  が素数であると検証した場合に、前記識別データに含まれるデータ  $IDKey$  と前記データ  $p$  と公開されているデータ  $M$  と

5 用いて  $(IDKey \cdot p \bmod M)$  を算出する第 2 の手段と、

前記第 2 の手段が算出した  $(IDKey \cdot p \bmod M)$  を基に得た復号鍵を用いて、前記記録媒体に記録された暗号データを復号する第 3 の手段と

を有するデータ処理装置。

23. 素数  $q_1$  と  $q_2$  の積であり公開されたデータを  $M$  とし、 $w$  を  $1 \leq w \leq W$  の整数とし、 $W$  ( $W \geq 2$ ) 個の異なるデータを  $e(w)$  とし、 $e(w)$  を巡回群  $Z * M$  の生成元とし、 $e(w)$  と  $\lambda(M)$  は互いに素であり、 $\lambda(M)$  を  $(q_1 - 1)$  と  $(q_2 - 1)$  との最小公倍数とした場合に、 $W$  個の記録媒体  $STM(w)$  の各々に割当てて識別データ  $ID(w)$  を生成するデータ処理方法であって、

巡回群  $Z * M$  の生成元であるデータ  $S$  と、 $\lambda(M)$  を法としたときの  $e(w)$  の逆数であるデータ  $d(w)$  と、上記データ  $M$  とを用いて、 $(S \cdot d(w) \bmod M)$  を算出する第 1 の工程と、

前記  $e(w)$  と前記第 1 の工程で算出した  $(S \cdot d(w) \bmod M)$  とを含む識別データ  $ID(w)$  を、記録媒体  $STM(w)$  に割当てて第 2 の工程とを有するデータ処理方法。

24. 上記データ  $S$  を暗号鍵として用いて暗号化された暗号データと、前記識別データ  $ID(w)$  とを前記記録媒体  $STM(w)$  に書き込む第 3 の工程をさらに有する請求項 23 に記載のデータ処理方法。

25. 素数  $q_1$  と  $q_2$  の積であり公開されたデータを  $M$  とし、 $w$  を  $1 \leq w \leq W$  の整数とし、 $W$  ( $W \geq 2$ ) 個の異なるデータを  $e(w)$  とし、 $e(w)$  を巡回群  $Z * M$  の生成元とし、 $e(w)$  と  $\lambda(M)$  は互いに素であり、 $\lambda(M)$  を  $(q_1 - 1)$  と  $(q_2 - 1)$  との最小公倍数とした場合に、 $W$  個の記録媒体  $STM(w)$  の各々



に割当てて識別データ  $ID(w)$  を生成するデータ処理装置が実行するプログラムであって、

巡回群  $Z * M$  の生成元であるデータ  $S$  と、 $\lambda(M)$  を法としたときの  $e(w)$  の逆数であるデータ  $d(w)$  と、上記データ  $M$  とを用いて、 $(S d(w) \bmod M)$

5 を算出する第1の手順と、

前記  $e(w)$  と前記第1の手順で算出した  $(S d(w) \bmod M)$  とを含む識別データ  $ID(w)$  を、記録媒体  $STM(w)$  に割当てて第2の手順とを有するプログラム。

26. 素数  $q_1$  と  $q_2$  の積であり公開されたデータを  $M$  とし、 $w$  を  $1 \leq w \leq W$  の整数とし、 $W$  ( $W \geq 2$ ) 個の異なるデータを  $e(w)$  とし、 $e(w)$  を巡回群  $Z * M$  の生成元とし、 $e(w)$  と  $\lambda(M)$  は互いに素であり、 $\lambda(M)$  を  $(q_1 - 1)$  と  $(q_2 - 1)$  との最小公倍数とした場合に、 $W$  個の記録媒体  $STM(w)$  の各々に割当てて識別データ  $ID(w)$  を生成するデータ処理装置であって、

巡回群  $Z * M$  の生成元であるデータ  $S$  と、 $\lambda(M)$  を法としたときの  $e(w)$  の逆数であるデータ  $d(w)$  と、上記データ  $M$  とを用いて、 $(S d(w) \bmod M)$  を算出する第1の手段と、

前記  $e(w)$  と前記第1の手段が算出した  $(S d(w) \bmod M)$  とを含む識別データ  $ID(w)$  を、記録媒体  $STM(w)$  に割当てて第2の手段とを有するデータ処理装置。

27. 記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理方法であって、

前記識別データに含まれるデータ  $e$  およびデータ  $I$  と公開されているデータ  $M$  とを用いて  $(I e \bmod M)$  を算出する第1の工程と、

前記第1の工程で算出した  $(I e \bmod M)$  を復号鍵として用いて、前記記録媒体に記録された暗号データを復号する第2の工程と

を有するデータ処理方法。

28. 記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置が実行するプログラムであって、

前記識別データに含まれるデータ  $e$  およびデータ  $I$  と公開されているデータ  $M$  と用いて  $(I \oplus e \oplus M)$  を算出する第1の手順と、

- 5 前記第1の手順で算出した  $(I \oplus e \oplus M)$  を復号鍵として用いて、前記記録媒体に記録された暗号データを復号する第2の手順とを有するプログラム。

29. 記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置であって、

- 10 前記識別データに含まれるデータ  $e$  およびデータ  $I$  と公開されているデータ  $M$  と用いて  $(I \oplus e \oplus M)$  を算出する第1の手段と、

前記第1の手が算出した  $(I \oplus e \oplus M)$  を復号鍵として用いて、前記記録媒体に記録された暗号データを復号する第2の手段とを有するデータ処理装置。

- 15 30. データを記録する記録媒体であって、

前記記録媒体の管理元の秘密鍵データを用いて生成され、前記管理元の公開鍵データを基に正当性が検証され、当該記録媒体を識別する識別データを記録した

記録媒体。

- 20 31. データを記録する記録媒体であって、

前記記録媒体の管理元の公開鍵データを用いて第1のデータを生成するために用いられる署名データと、前記第1のデータと比較して識別データの正当性を検証するために用いられる第2のデータとを含み前記記録媒体を識別する前記識別データを記録した

- 25 記録媒体。

32. 暗号データを記録する記録媒体であって、

素数であるデータ  $p$  と、

前記暗号データを復号するために用いられるコンテンツ鍵データである  
( $IDKey_p \bmod M$ ) を前記データ  $p$  と公開されているデータ  $M$  と共に算  
出するために用いられるデータ  $IDKey$  と

- 5        を含み前記記録媒体を識別する識別データを記録した  
記録媒体。

33.    暗号データを記録する記録媒体であって、

- 前記暗号データを復号するために用いられるコンテンツ鍵データである  
( $Ie \bmod M$ ) を、公開されているデータ  $M$  と共に算出するために用いられ  
10    るデータ  $e$  およびデータ  $I$  とを含み前記記録媒体を識別する識別データを記録し  
た  
記録媒体。

FIG. 1

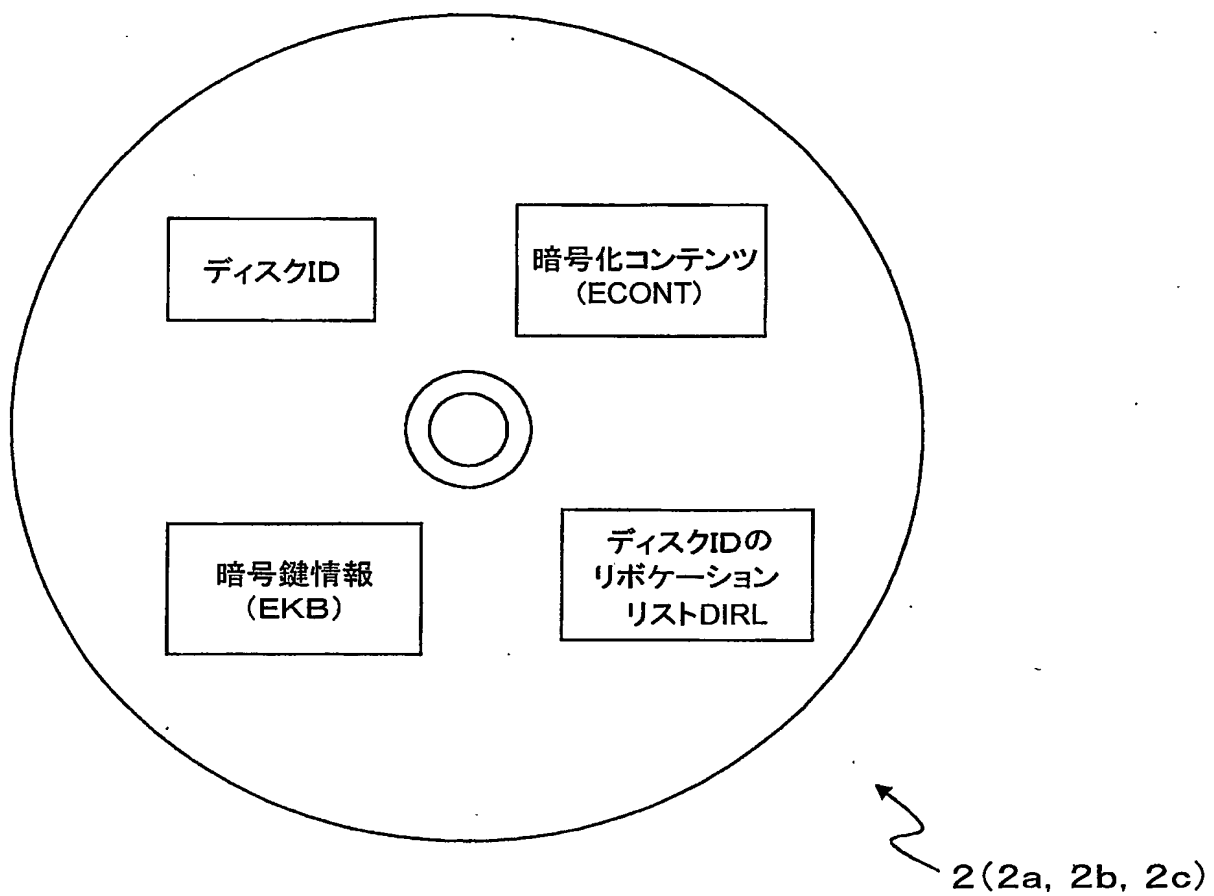


FIG. 2

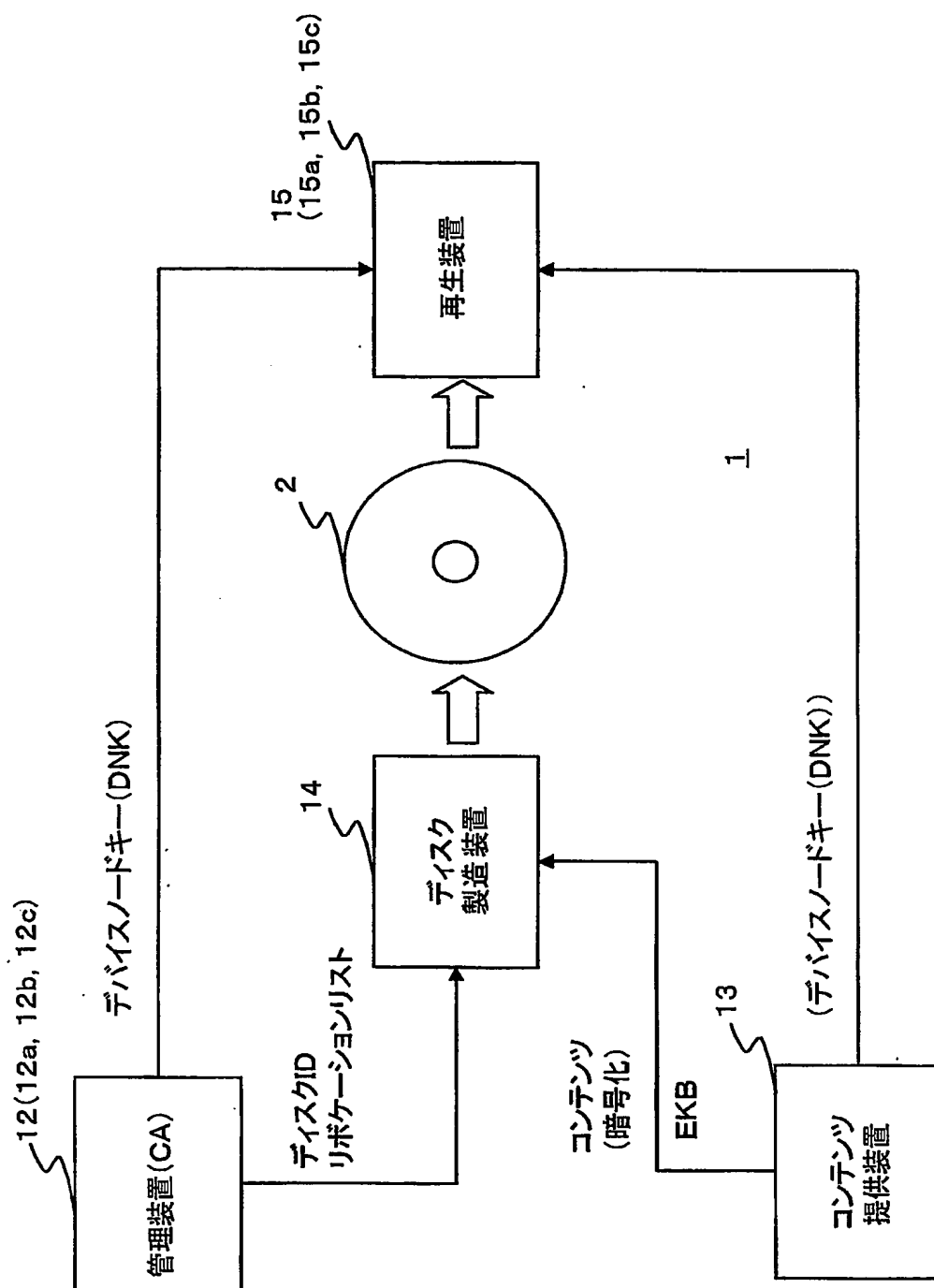


FIG. 3

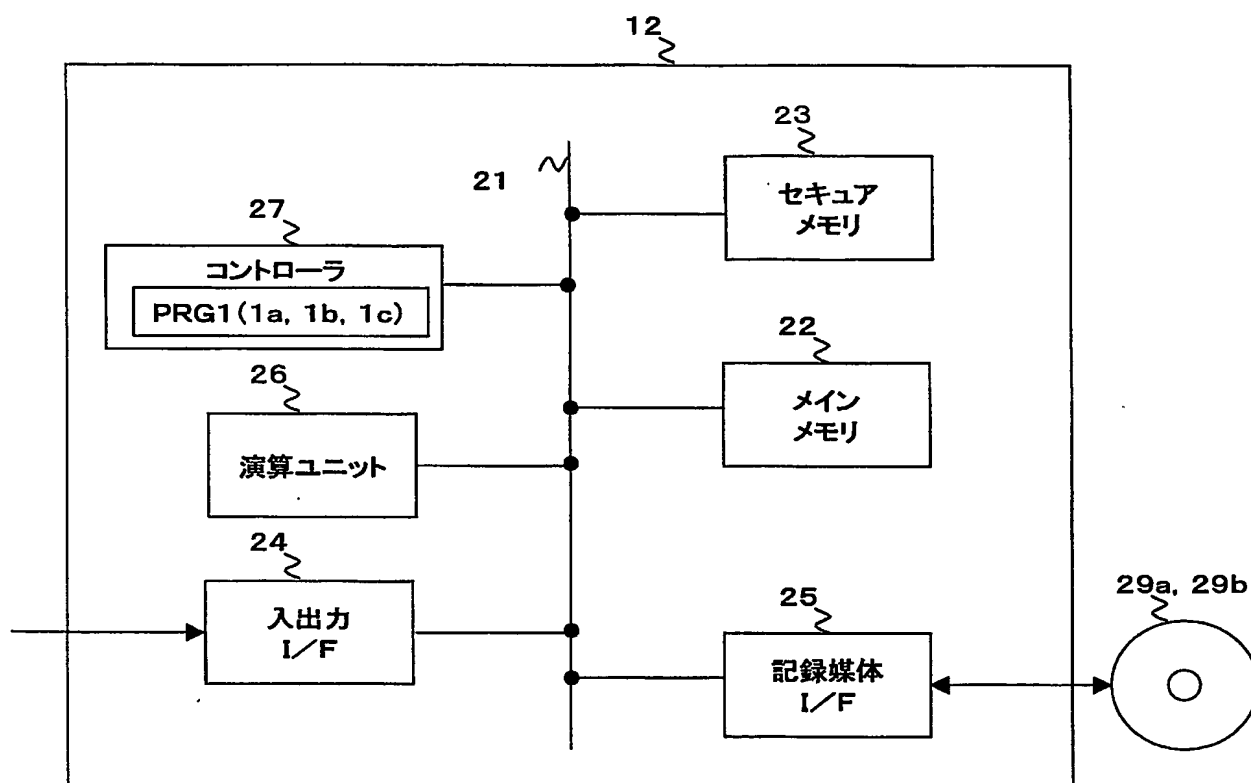


FIG. 4

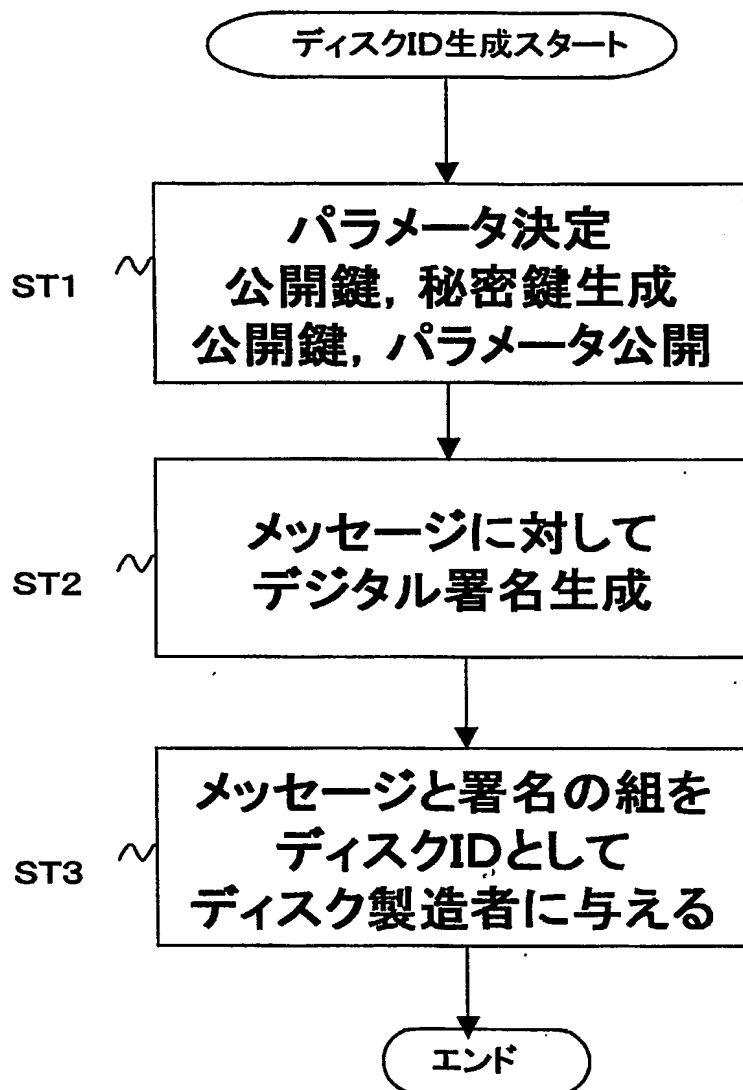


FIG. 5

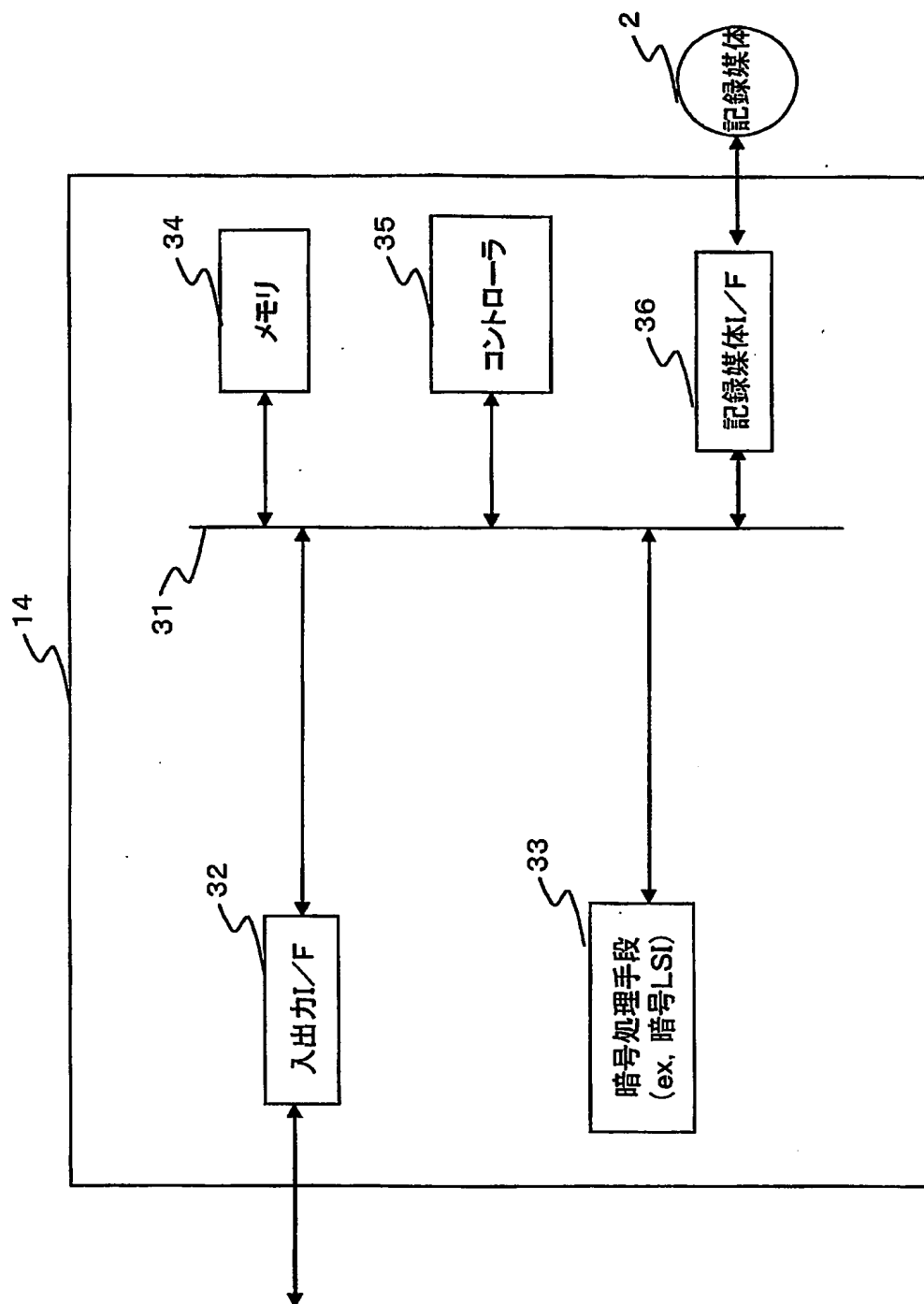




FIG. 6

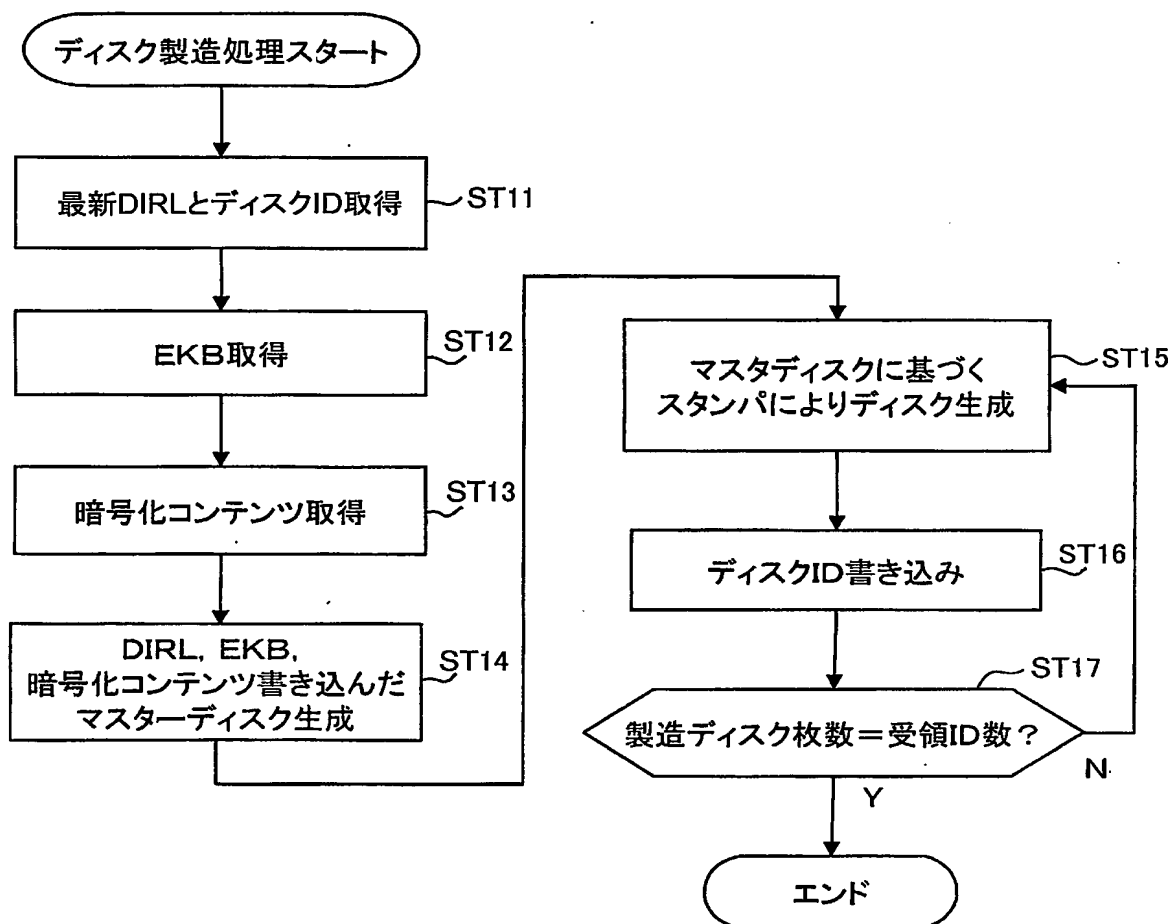


FIG. 7

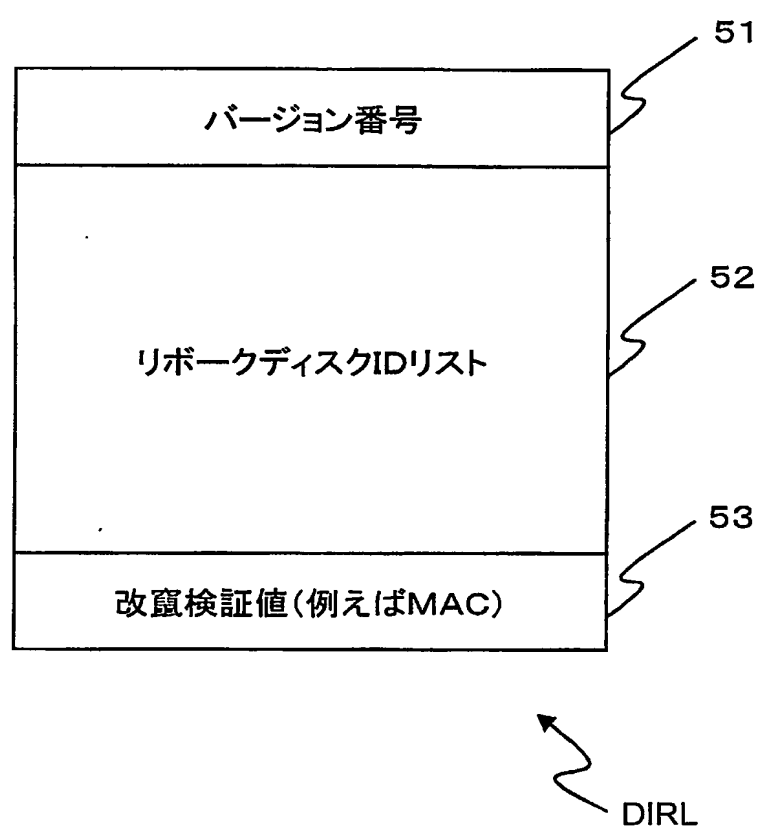


FIG. 8

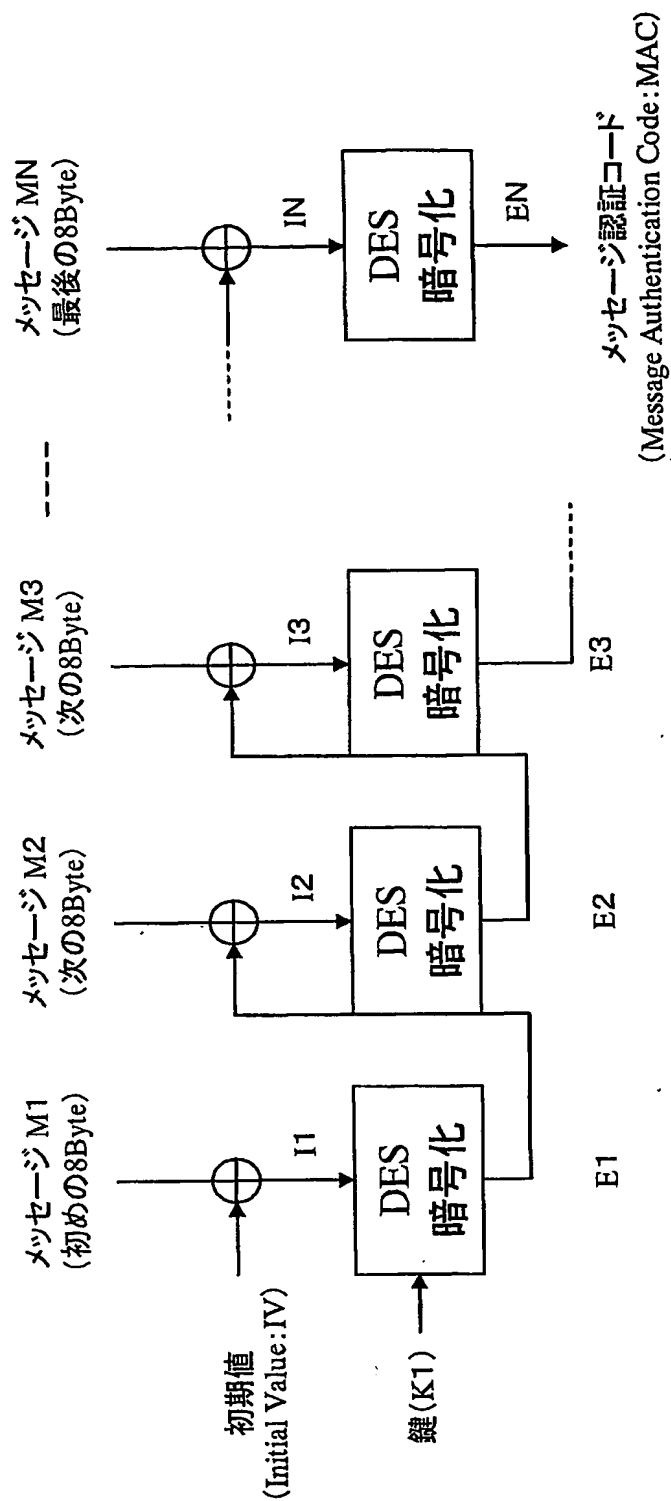


FIG. 9

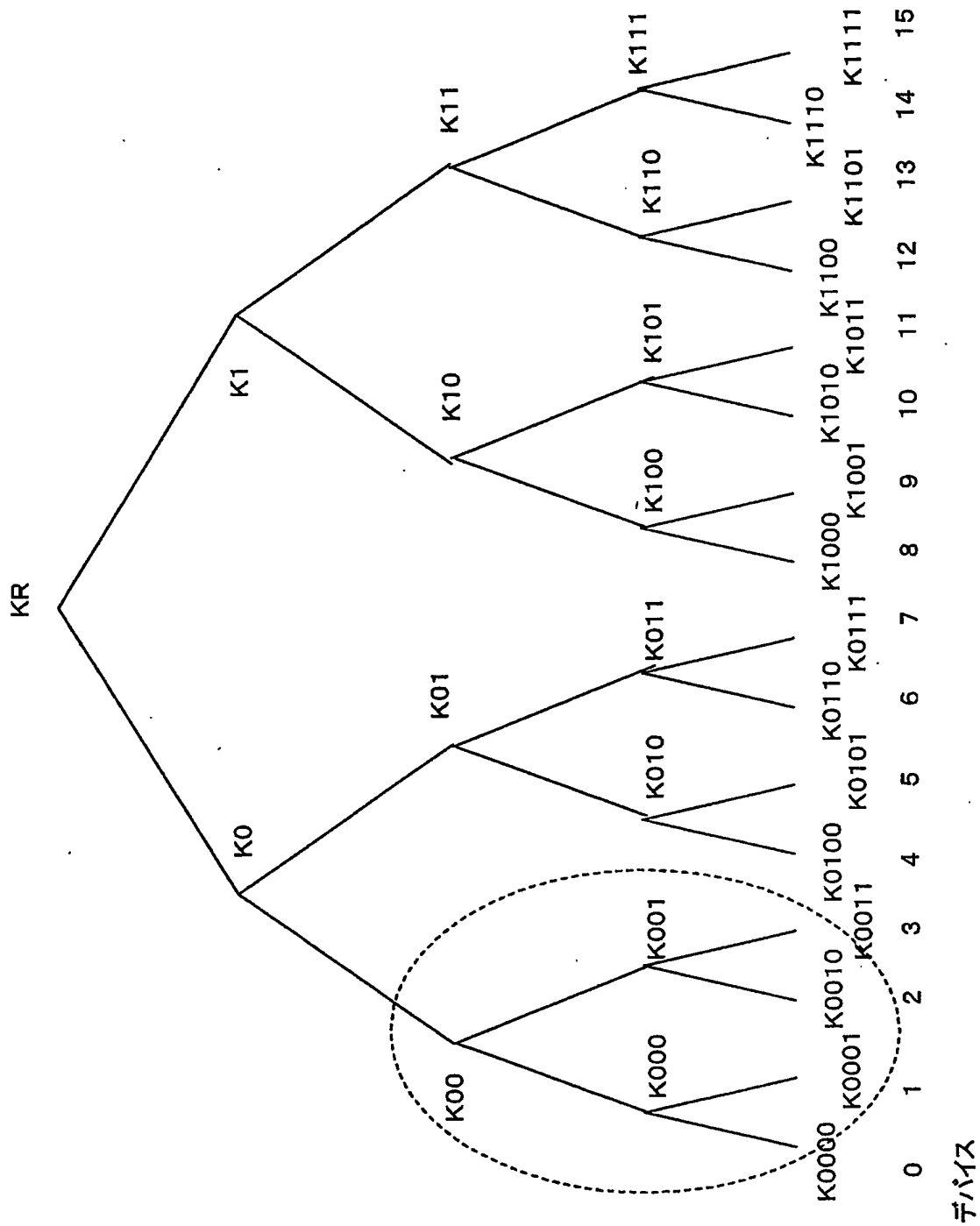


FIG. 10A

有効化キーブロック

(EKB:Enabling Key Block)例1

デバイス0, 1, 2にバージョン:tのノードキーを送付

バージョン(Version): t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

FIG. 10B

有効化キーブロック

(EKB:Enabling Key Block) 例2

デバイス0, 1, 2にバージョン:tのノードキーを送付

バージョン(Version): t	
インデックス	暗号化キー
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

FIG. 11

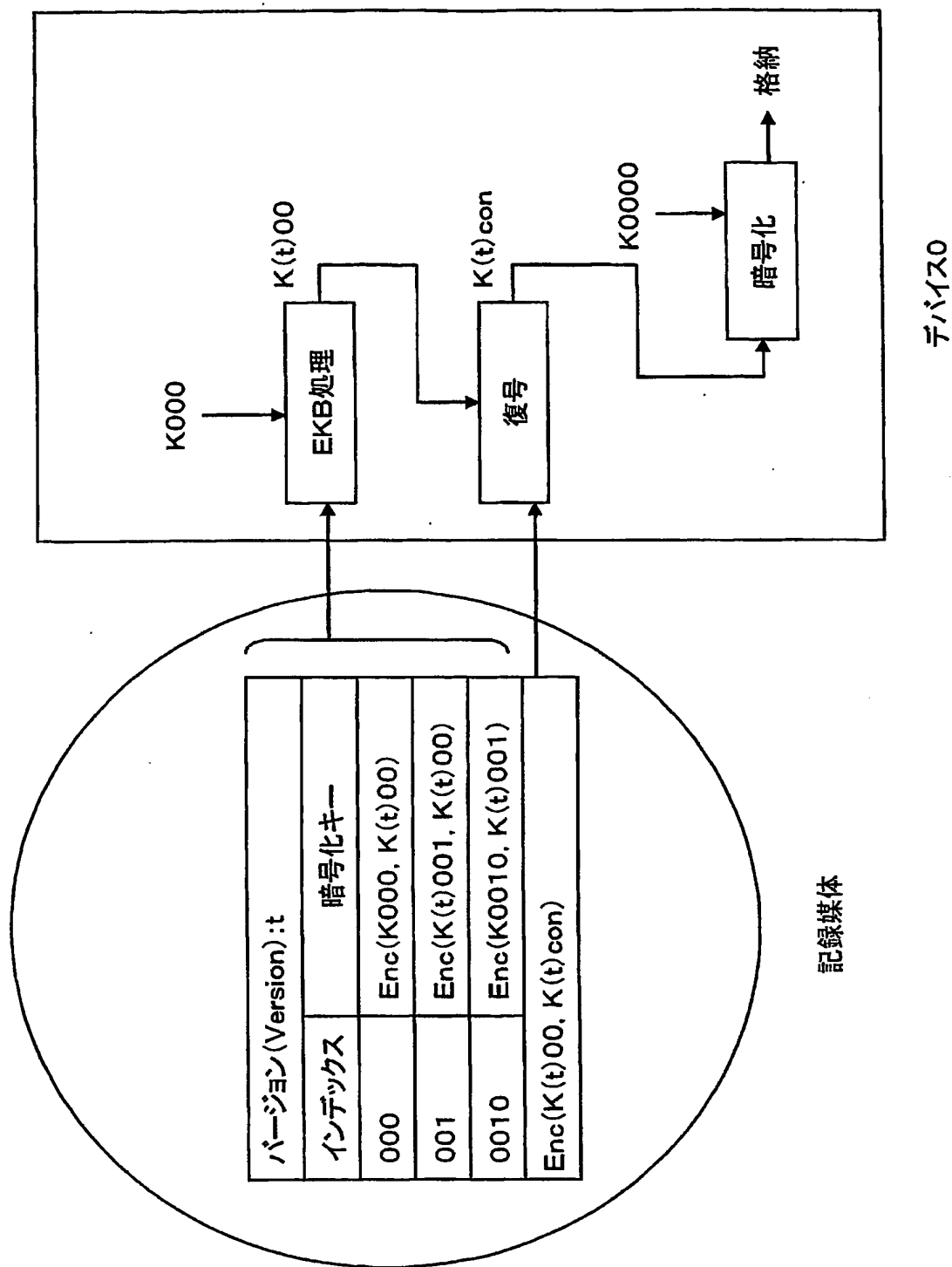


FIG. 12

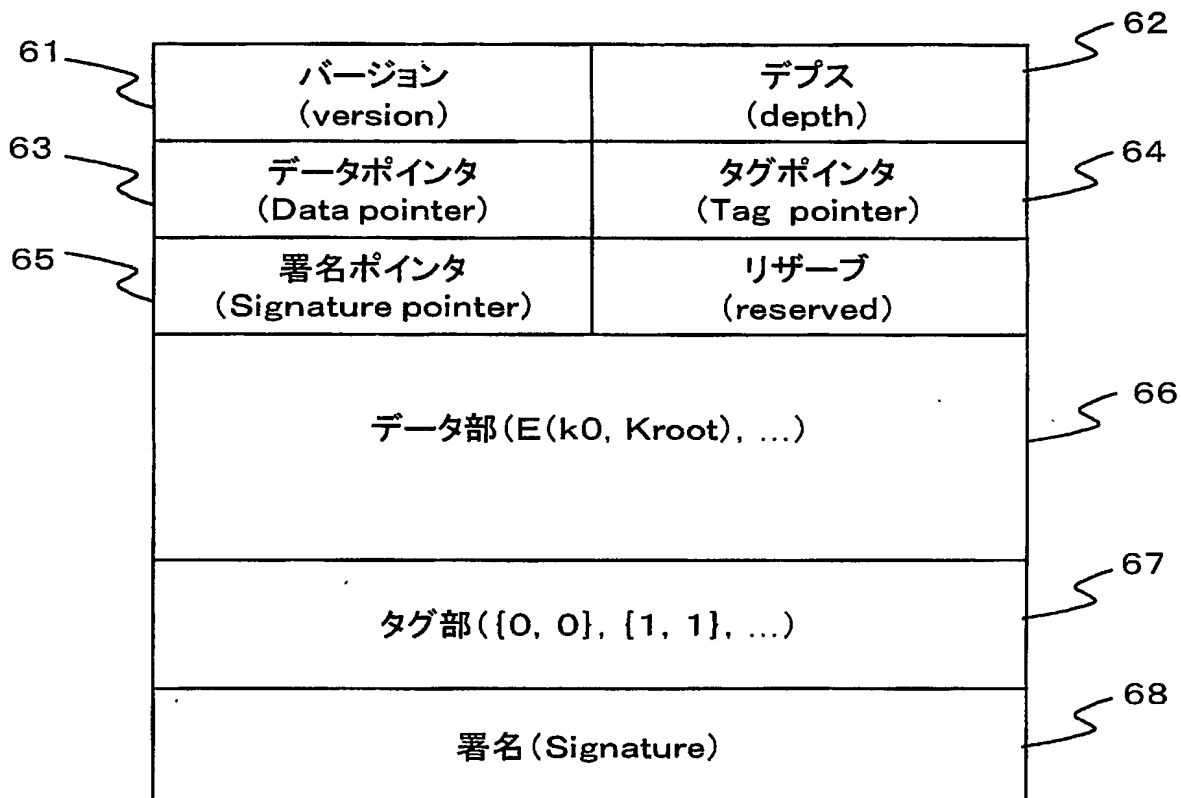


FIG. 13A

FIG. 13B

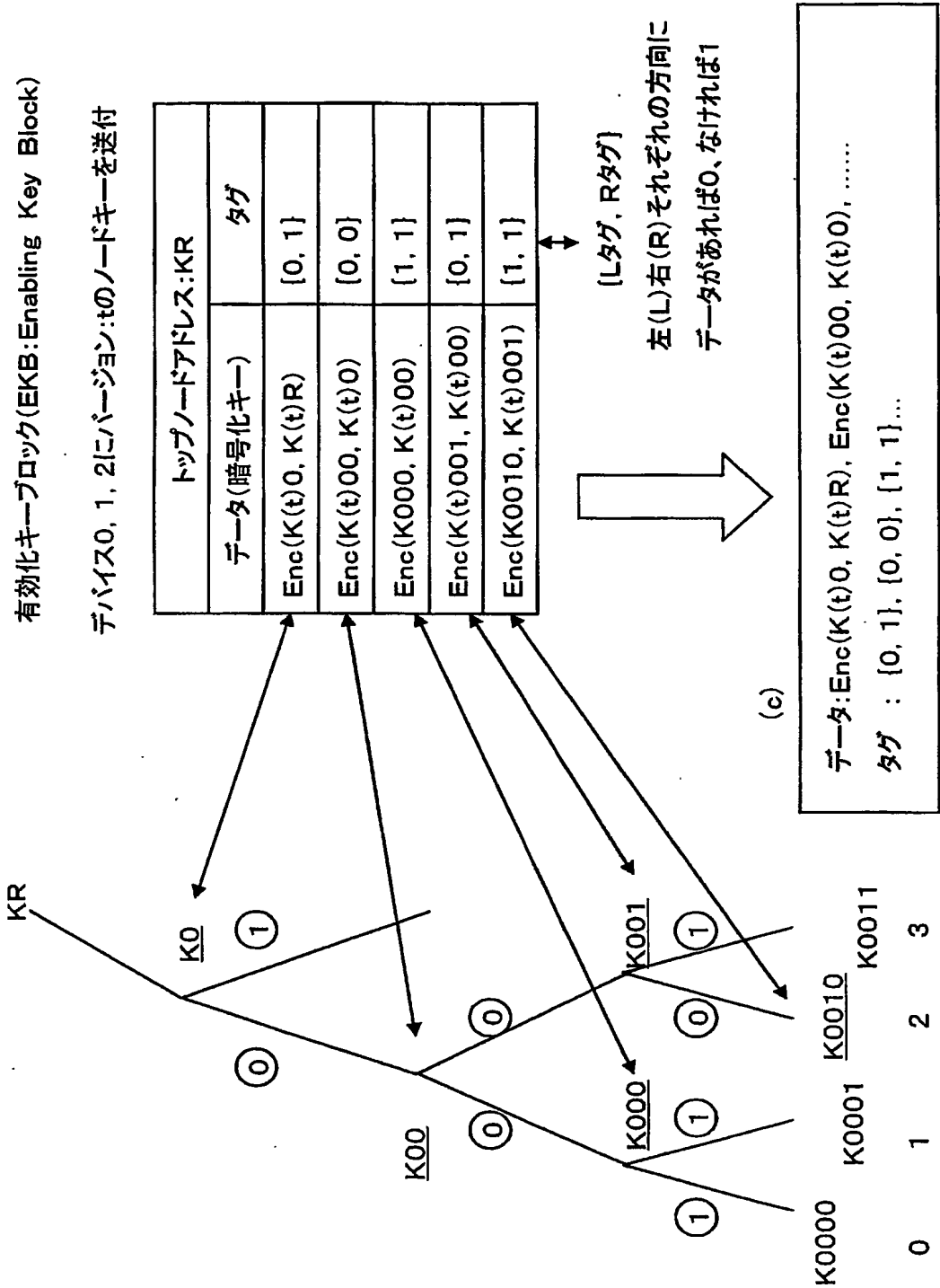




FIG. 14

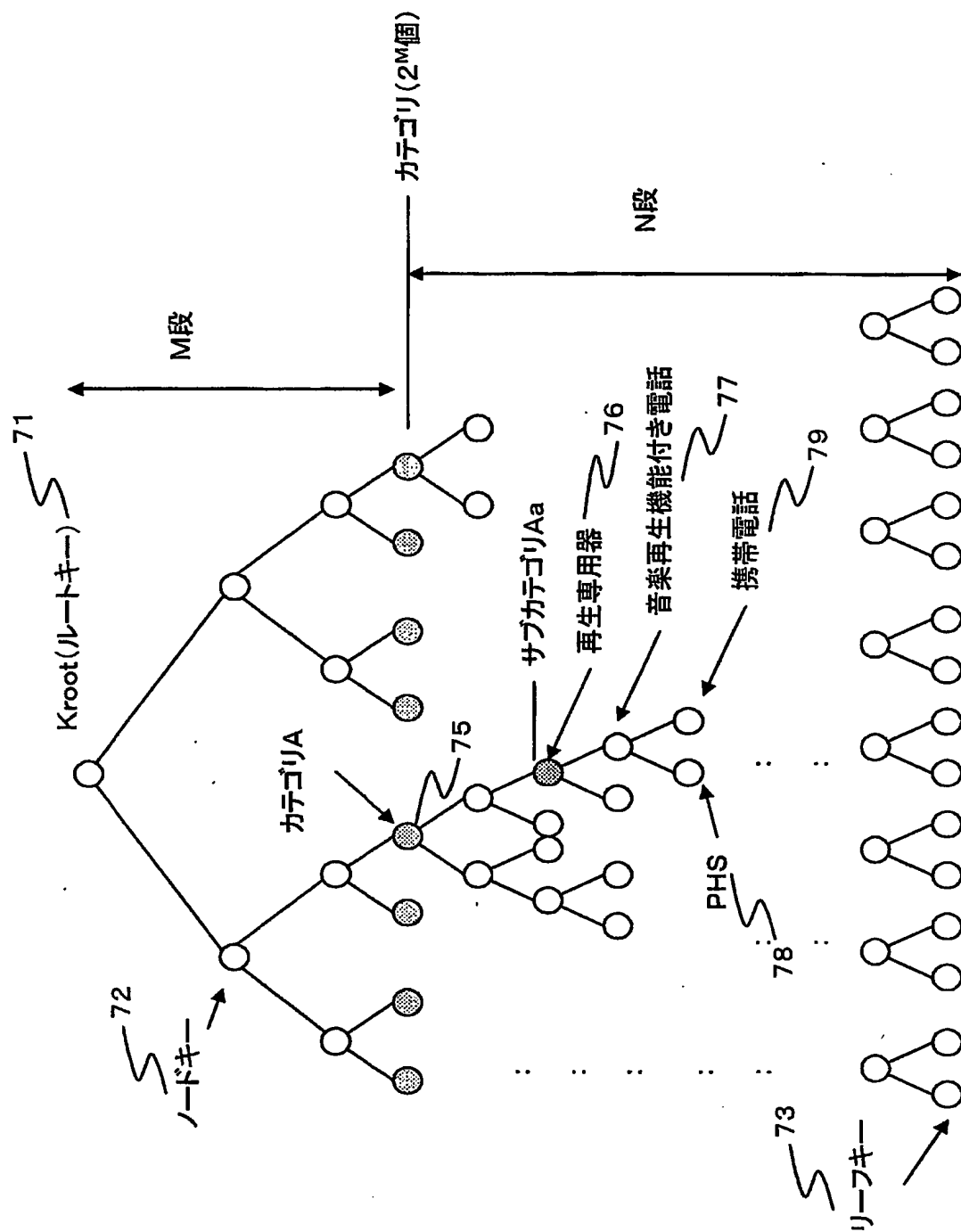


FIG. 15

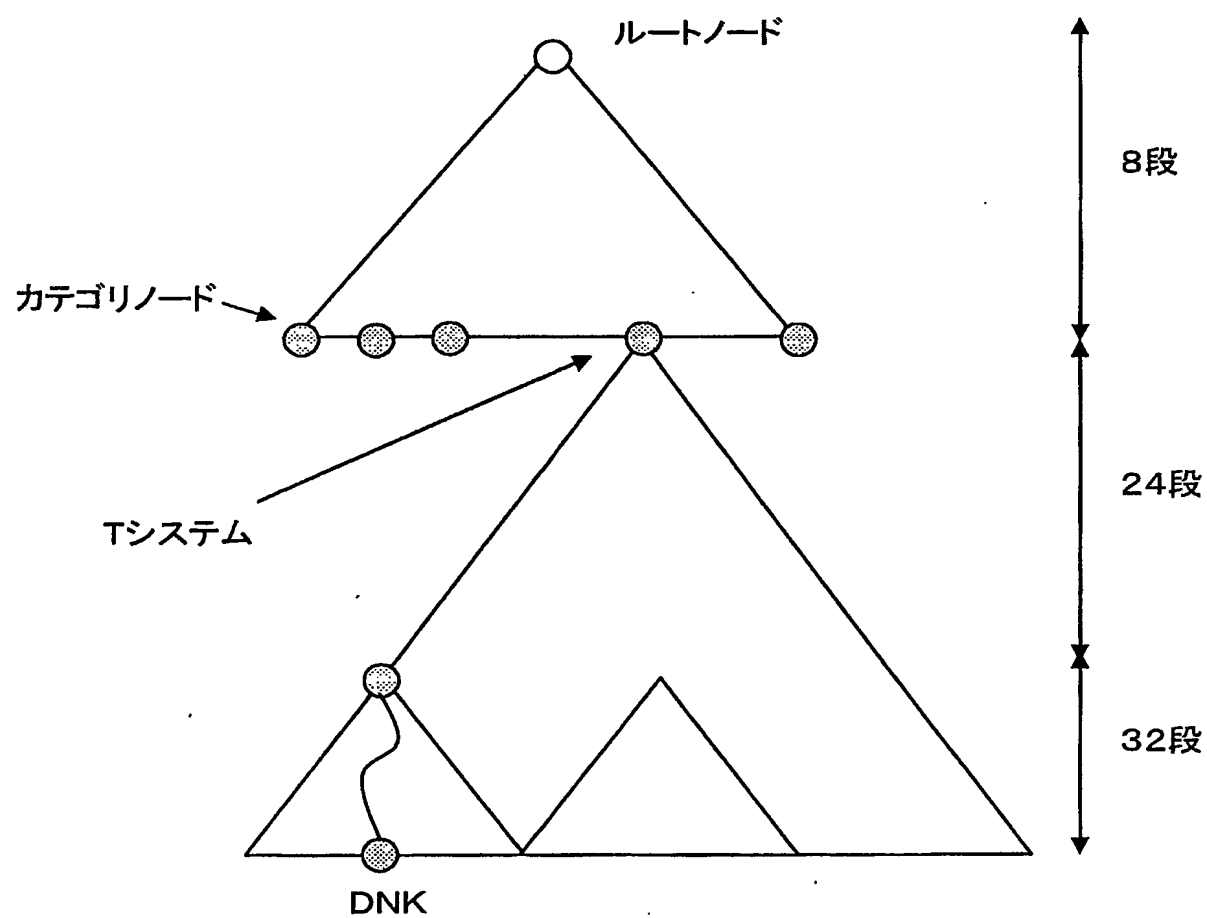


FIG. 16

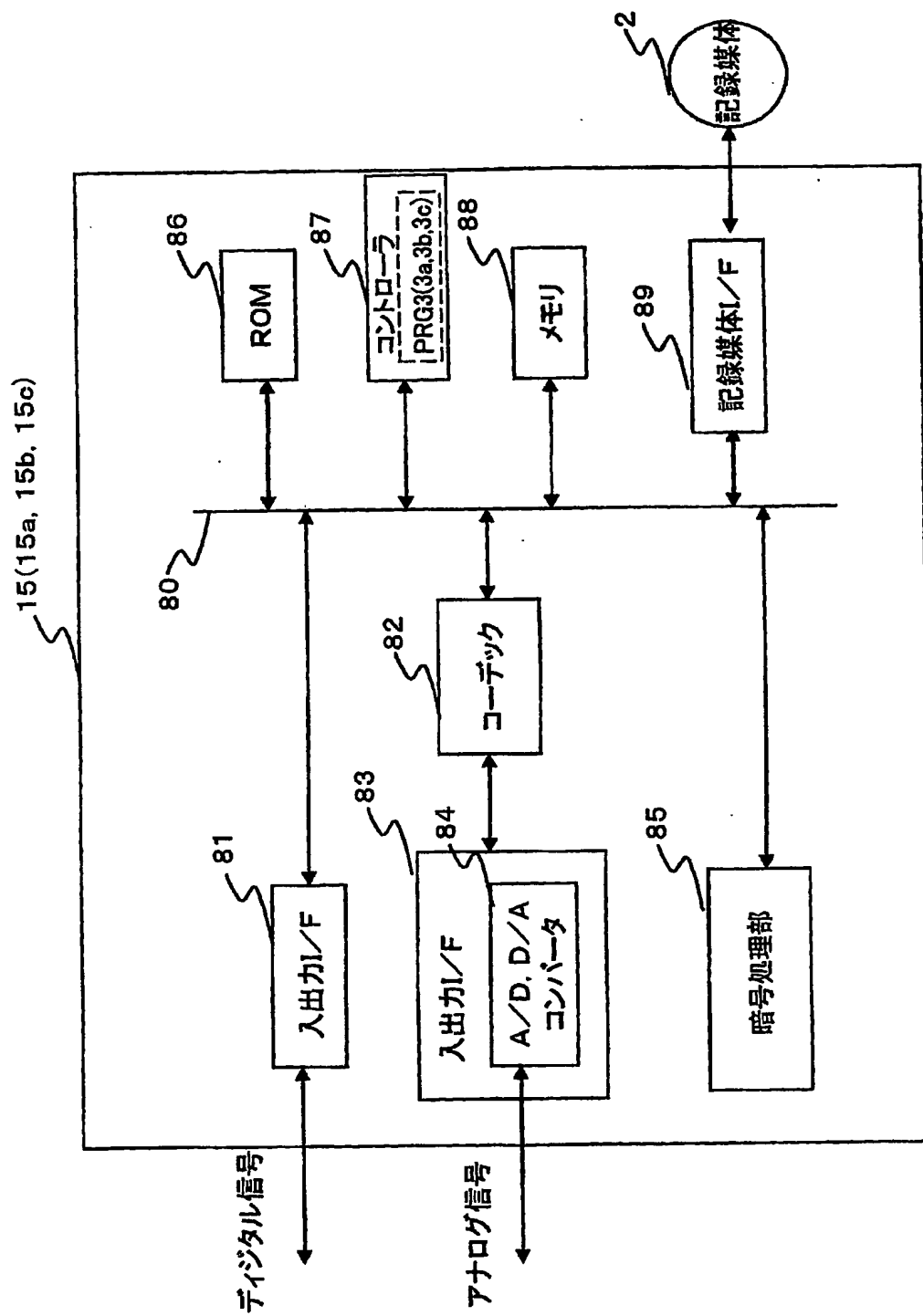


FIG. 17

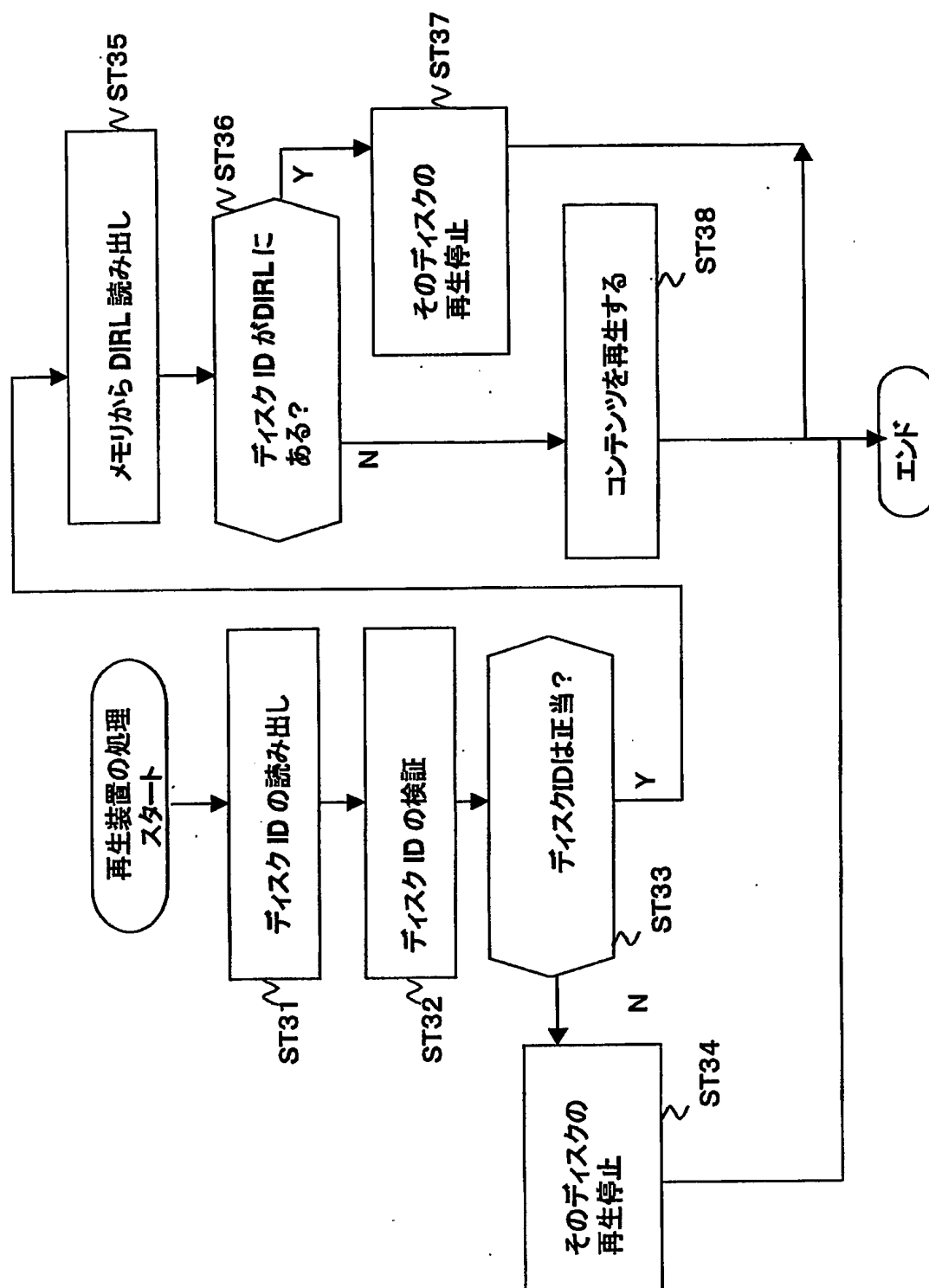


FIG. 18

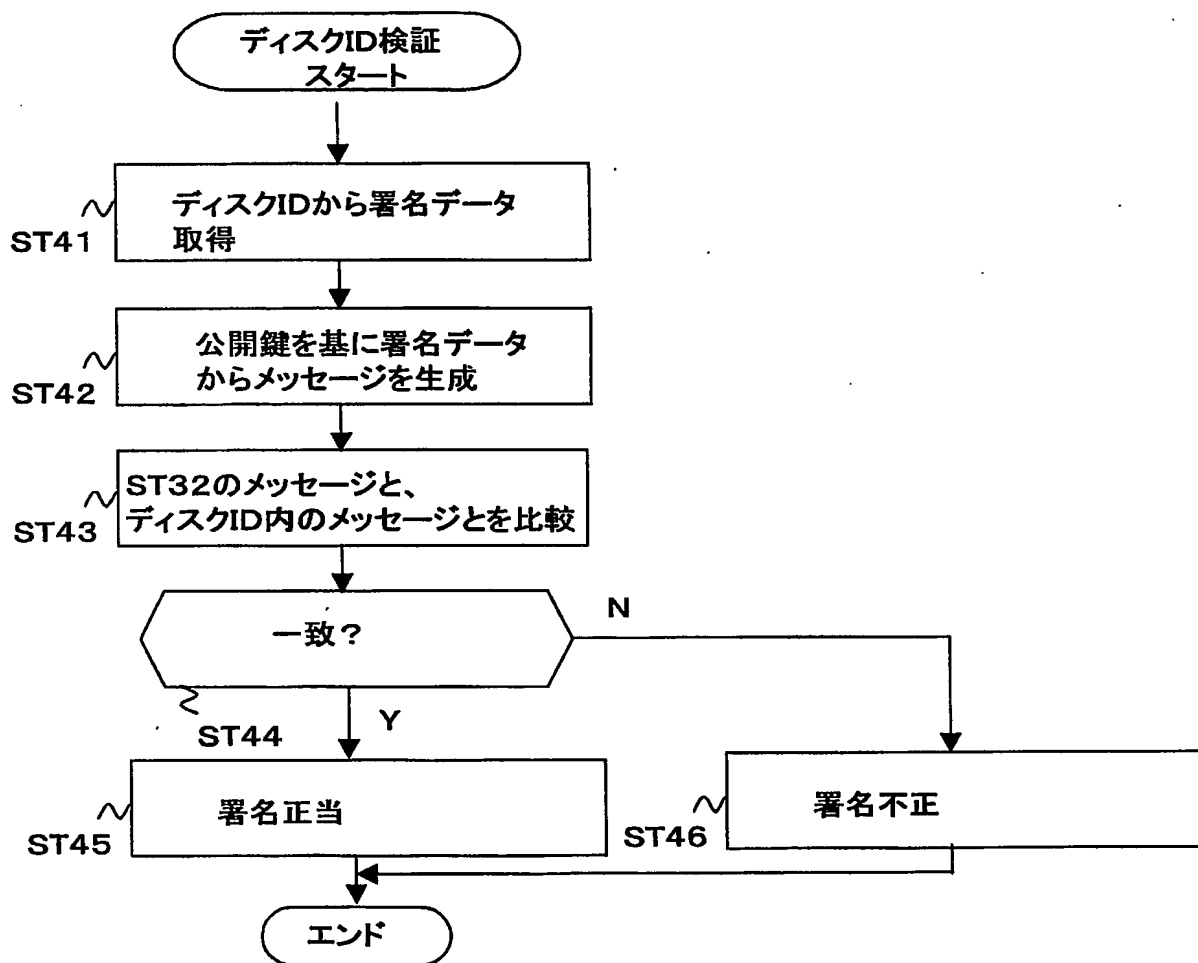


FIG. 19

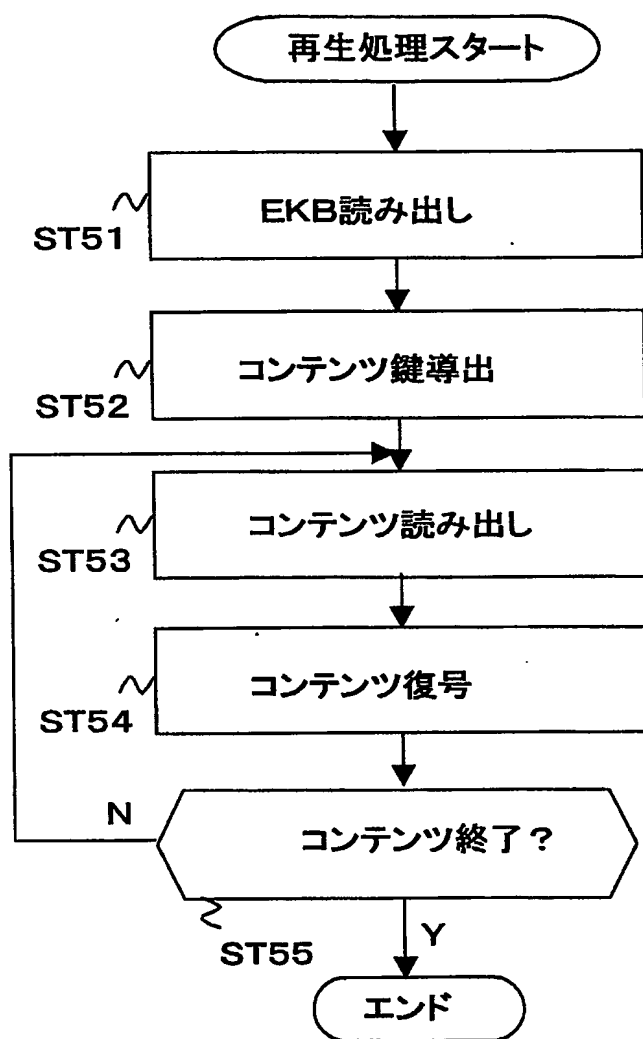


FIG. 20

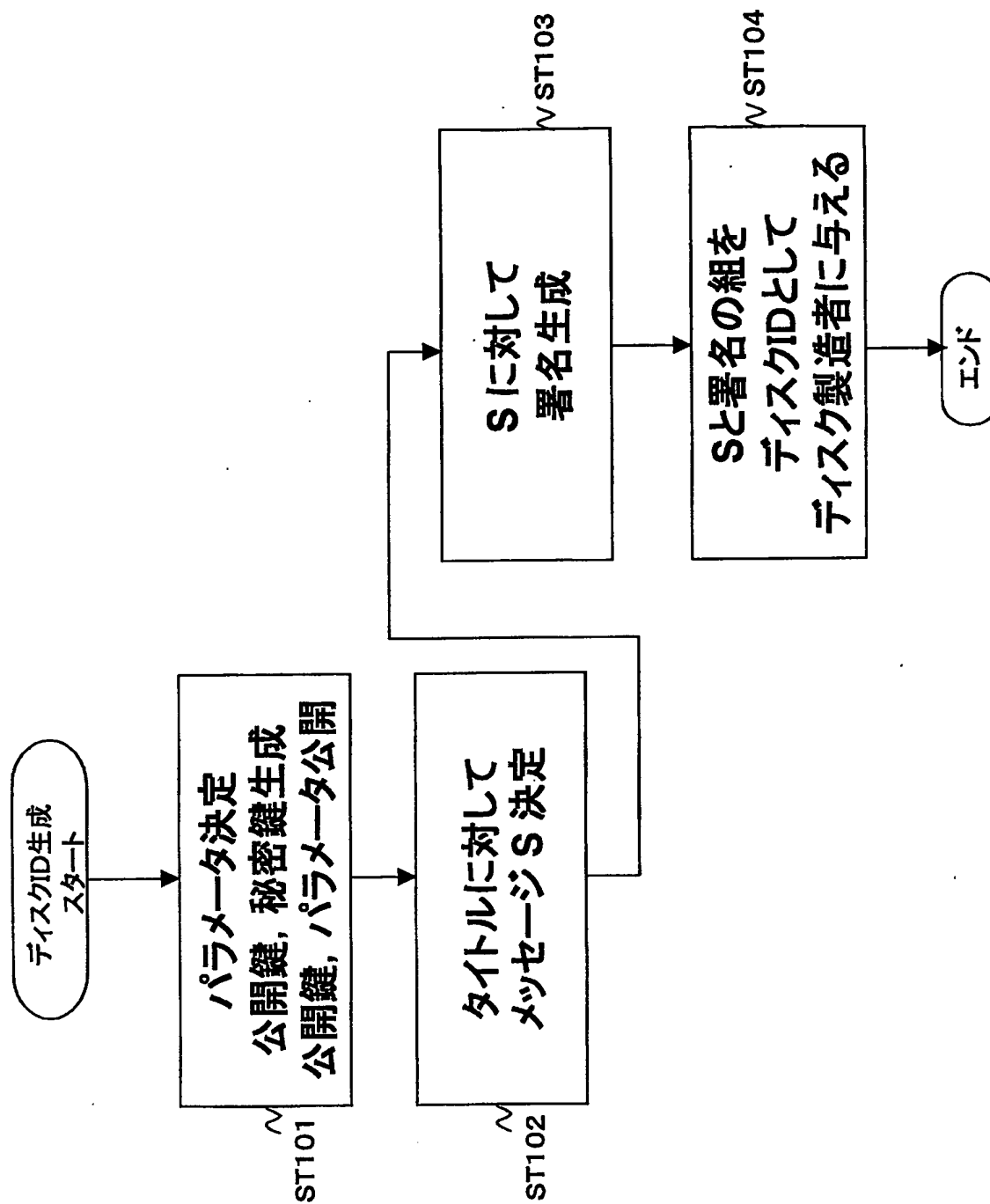


FIG. 21

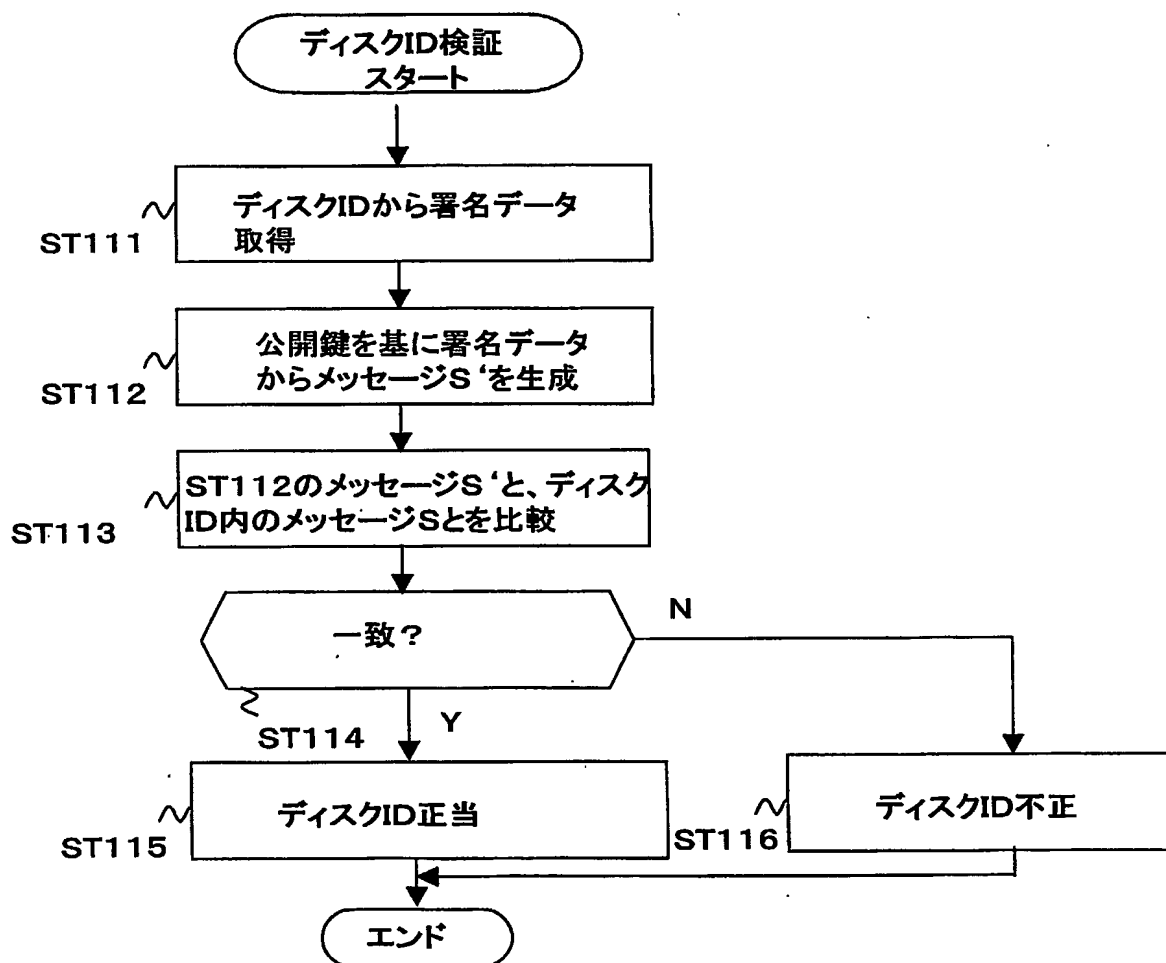




FIG. 22

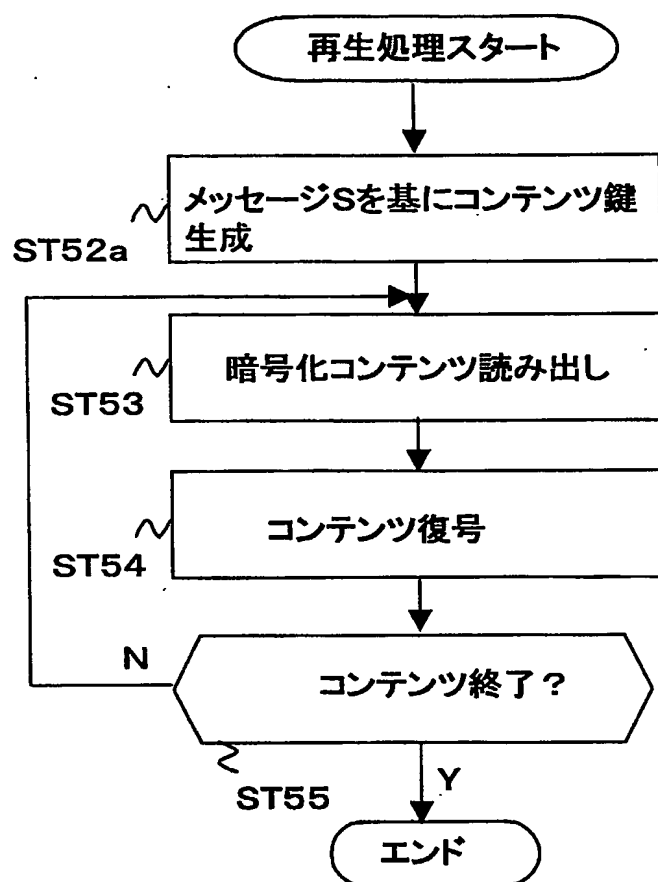


FIG. 23

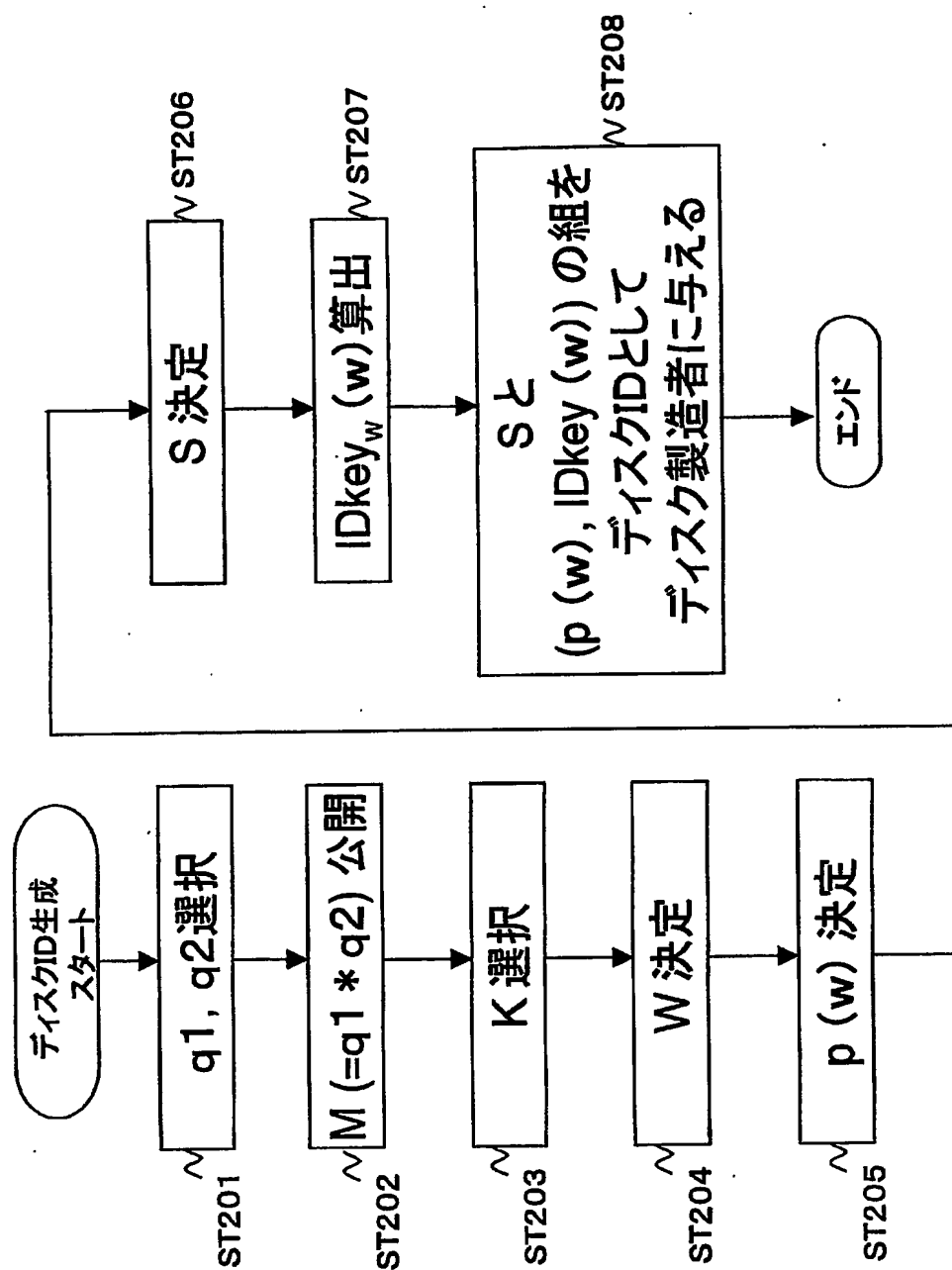


FIG. 24

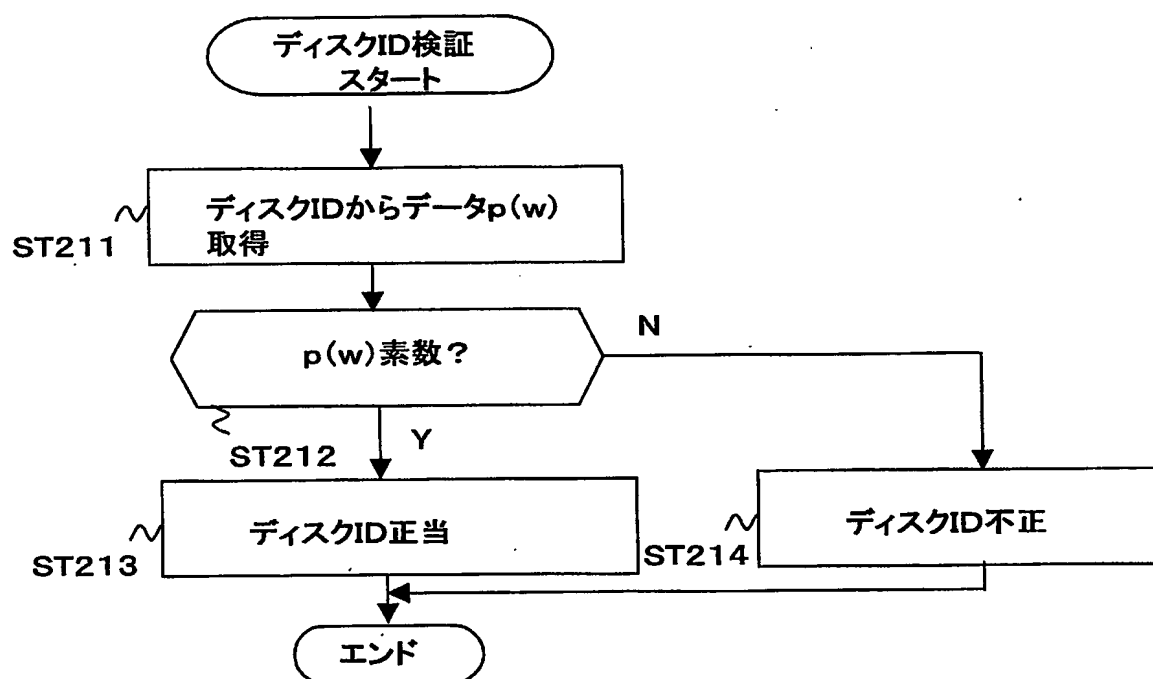


FIG. 25

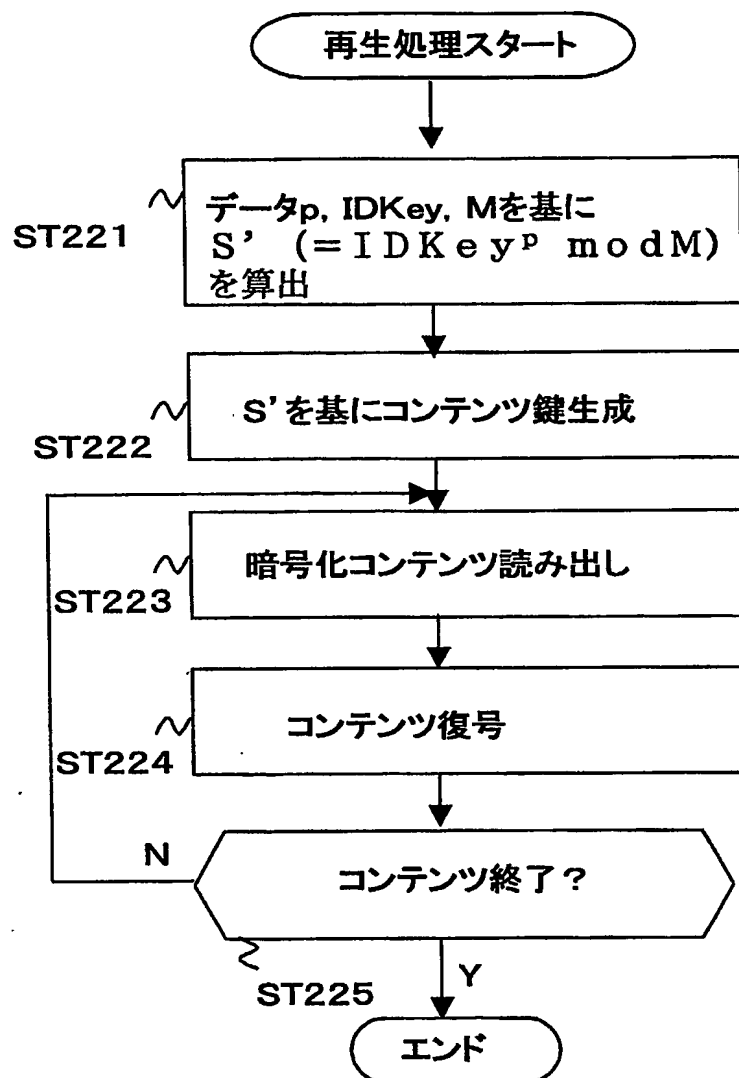


FIG. 26

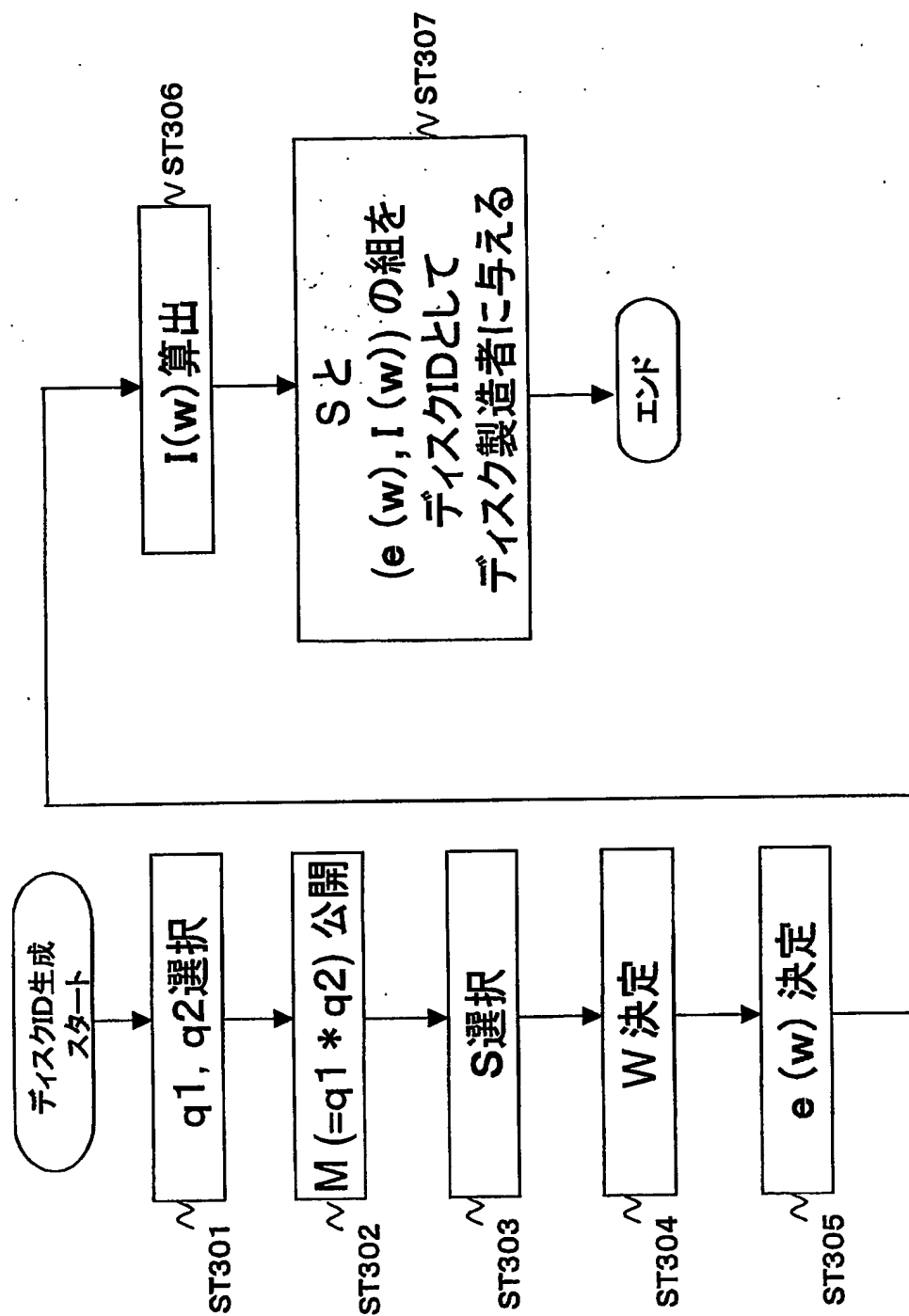
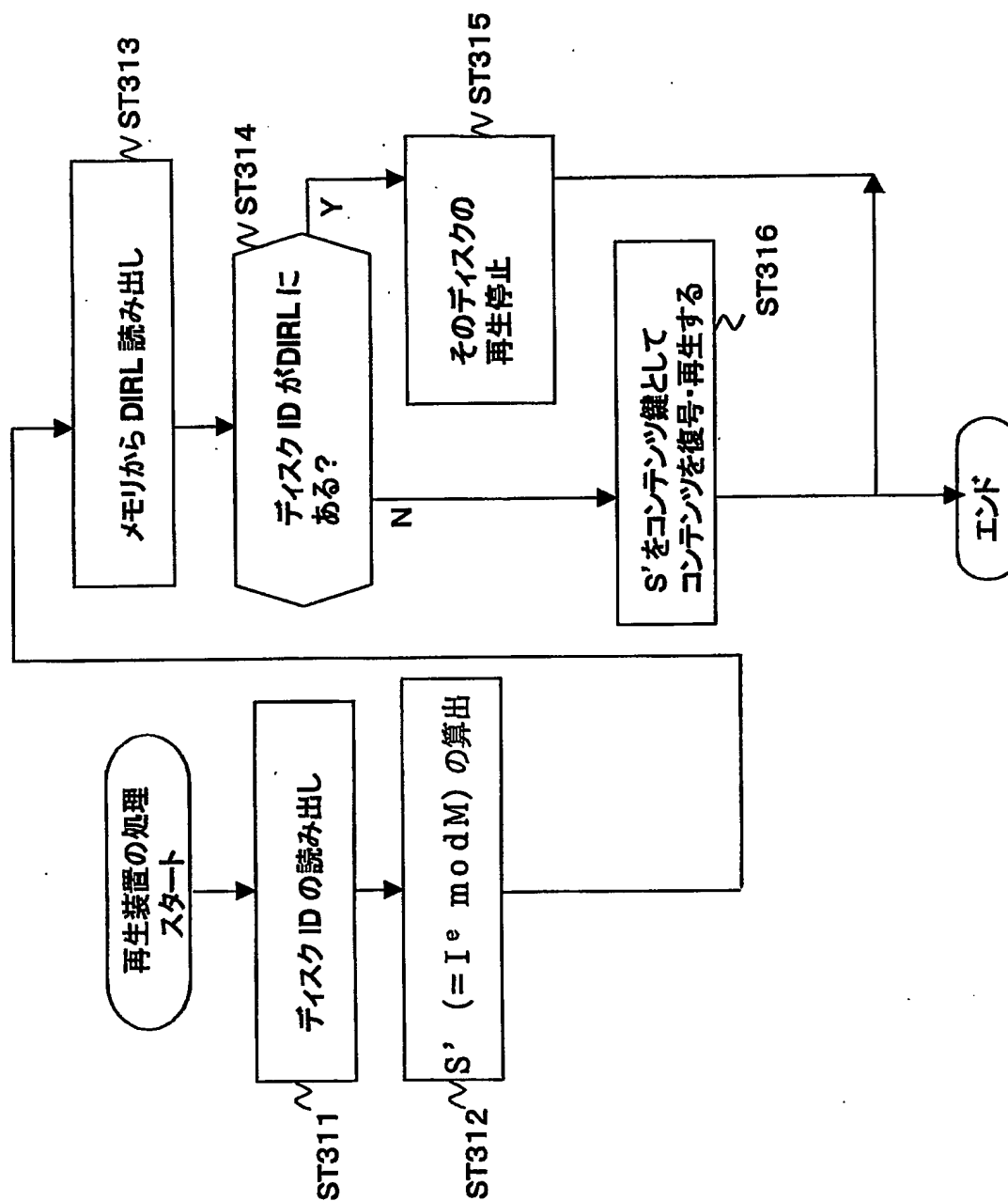


FIG. 27



## 符 号 の 説 明

- 2, 2 a, 2 b, 2 c…ディスク型記録媒体
- 1 2, 1 2 a, 1 2 b, 1 2 c…管理装置
- 5 1 3…コンテンツ提供装置
- 1 4…ディスク製造装置
- 1 5, 1 5 a, 1 5 b, 1 5 c…再生装置
- 2 1…バス
- 2 2…メインメモリ
- 10 2 3…セキュアメモリ
- 2 4…入出力インタフェース
- 2 5…記録媒体インタフェース
- 2 6…演算ユニット
- 2 7…コントローラ
- 15 8 0…バス
- 8 1…入出力インタフェース
- 8 2…コーデック
- 8 3…入出力インタフェース
- 8 4…コンバータ
- 20 8 5…暗号処理部
- 8 6…ROM
- 8 7…コントローラ
- 8 8…メモリ
- 8 9…記録媒体インタフェース

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/006324

## A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl<sup>7</sup> G11B20/10, G11B20/12, G11B27/00, G06F12/14, H04L9/00, H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>7</sup> G11B20/10, G11B20/12, G11B27/00, G06F12/14, H04L9/00, H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2004

Kokai Jitsuyo Shinan Koho 1971-2004 Jitsuyo Shinan Toroku Koho 1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2002-132457 A (Victor Company Of Japan, Ltd.), 10 May, 2002 (10.05.02), Full text; Figs. 1 to 11 (Family: none)	1-4, 9-12, 16-19, 23-26
X	JP 11-212454 A (NHK Spring Co., Ltd.), 06 August, 1999 (06.08.99), Full text; Figs. 1 to 10 (Family: none)	1-4, 9-12, 6-19, 23-26
X	JP 11-202766 A (Canon Inc.), 30 July, 1999 (30.07.99), Full text; Figs. 1 to 5 & US 6298153 B1	1-4, 9-12, 16-19, 23-26

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search  
02 September, 2004 (02.09.04)

Date of mailing of the international search report  
21 September, 2004 (21.09.04)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.



**INTERNATIONAL SEARCH REPORT**

International application No.

PCT/JP2004/006324

**Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)**

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:  
because they relate to subject matter not required to be searched by this Authority, namely:
  
2. ☐ Claims Nos.:  
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
  
3. ☐ Claims Nos.:  
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

**Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)**

This International Searching Authority found multiple inventions in this international application, as follows:

This application does not satisfy the requirement of unity of invention because of the reason given on the extra sheet.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.: 1-4, 9-12, 16-19, 23-26

**Remark on Protest**

- ☐ The additional search fees were accompanied by the applicant's protest.  
☐ No protest accompanied the payment of additional search fees.

Continuation of Box No.III of continuation of first sheet(2)

The inventions of claims 1-4, 9-12, 16-19, 23-26 have "a special technical feature" relating to "assigning a plurality of signature data to a plurality of different recording media."

The inventions of claims 5-8, 13-15, 20-22, 27-31 have "a special technical feature" relating to "authentication of validity of the identification data assigned to the recording medium."

The inventions of claims 32-33 have "a special technical feature" relating to "a recording medium for recording encrypted data and recording identification data identifying the recording medium containing the content key data."

Recording predetermined identification data on a recording medium so as to prevent unauthorized copying is a known configuration. And the public key encryption method using a secret key and a public key is a known technique.

Accordingly, these inventions have only the known configurations and are not so linked as to have a special technical feature.

There is no technical relationship among those inventions involving one or more of the same or corresponding technical features. Consequently, the inventions are not so linked as to form a single general inventive concept.

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> G11B 20/10 G11B 20/12 G11B 27/00  
G06F 12/14 H04L 9/00 H04L 9/32

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> G11B 20/10 G11B 20/12 G11B 27/00  
G06F 12/14 H04L 9/00 H04L 9/32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年  
日本国公開実用新案公報 1971-2004年  
日本国登録実用新案公報 1994-2004年  
日本国実用新案登録公報 1996-2004年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	J P 2002-132457 A (日本ビクター株式会社) 2002. 05. 10 , 全文, 第1-11図 (ファミリーなし)	1-4, 9-12, 16 -19, 23-26
X	J P 11-212454 A (日本発条株式会社) 1999. 08. 06 , 全文, 第1-10図 (ファミリーなし)	1-4, 9-12, 16 -19, 23-26

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの  
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
「O」 口頭による開示、使用、展示等に言及する文献  
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
「&」 同一パテントファミリー文献

国際調査を完了した日

02. 09. 2004

国際調査報告の発送日

21. 9. 2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)  
郵便番号100-8915  
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

前田 祐希

5Q

2946

電話番号 03-3581-1101 内線 3590

C (続き) 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	JP 11-202766 A (キャノン株式会社) 1999. 07. 30 , 全文, 第1-5図 & U.S. 6298153 B1	1-4, 9-12, 16 -19, 23-26

## 第Ⅱ欄 請求の範囲の一部の調査ができないときの意見 (第1ページの2の続き)

法第8条第3項 (PCT 17条(2)(a)) の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 \_\_\_\_\_ は、この国際調査機関が調査をすることを要しない対象に係るものである。  
つまり、
2. ☐ 請求の範囲 \_\_\_\_\_ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求の範囲 \_\_\_\_\_ は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

## 第Ⅲ欄 発明の単一性が欠如しているときの意見 (第1ページの3の続き)

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

単一性を満たさない理由は、特別ページに記載した。

1. ☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☒ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

請求の範囲 1-4, 9-12, 16-19, 23-26

## 追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。  
☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

請求の範囲1-4、9-12、16-19、23-26の「特別な技術的特徴」は、「複数の署名データを識別データとして異なる複数の記録媒体にそれぞれ割当てて」ることに関するものである。

請求の範囲の5-8、13-15、20-22、27-31の「特別な技術的特徴」は、「記録媒体に割当てられた識別データの正当性を検証する」ことに関するものである。

請求の範囲の32-33の「特別な技術的特徴」は「暗号データを記録する記録媒体であって、コンテンツ鍵データを含む記録媒体を識別する識別データを記録する」ことに関するものである。

不正コピーを防止するために、記録媒体に所定の識別データを記録することは、周知の構成である。そして、秘密鍵、公開鍵を用いる公開鍵暗号化方式は、周知技術である。

よって、これらの発明は、上記の周知の構成のみでそれぞれの発明が特別な技術的特徴を含む関係があるとは認められない。

よって、これらの発明は、一又は二以上の同一又は対応する特別な技術的特徴を含む技術的な関係にないから、単一の一般的発明概念を形成するように連関しているものとは認められない。